

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-164881  
(43)Date of publication of application : 07.06.2002

(51)Int.Cl. H04L 9/08  
G06F 13/00  
G09C 1/00  
H04L 9/32

(21)Application number : 2000-362913 (71)Applicant : SANYO ELECTRIC CO LTD  
FUJITSU LTD  
PFU LTD  
HITACHI LTD  
NIPPON COLUMBIA CO LTD

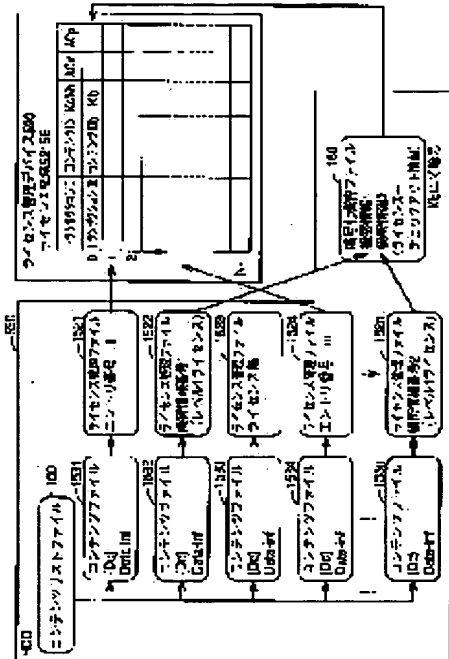
(22)Date of filing : 29.11.2000 (72)Inventor : HORI YOSHIHIRO  
KAMIMURA TORU  
HATAKEYAMA TAKAHISA  
TAKAHASHI MASATAKA  
TSUNEHIRO TAKASHI  
OMORI YOSHIO

(54) DATA TERMINAL DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a data terminal device, which can move encrypted contents data and license distributed by software to other data terminal devices.

SOLUTION: A hard disc 530 in a personal computer has a contents list file 150 and an encrypted confidential file 160. A license management device 520 stores a binding key Kb into a license area 5215B of memory. The encrypted confidential file 160 can be decoded and encrypted by the binding key Kb stored in the license management device 520. The acquired license for the encrypted content data is stored in the encrypted confidential file 160 as confidential information.



LEGAL STATUS

- [Date of request for examination]
- [Date of sending the examiner's decision of rejection]
- [Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
- [Date of final disposal for application]
- [Patent number]
- [Date of registration]
- [Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C): 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-164881

(P2002-164881A)

(43) 公開日 平成14年6月7日(2002.6.7)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テマコード*(参考)
H 0 4 L 9/08		G 0 6 F 13/00	5 4 0 S 5 J 1 0 4
G 0 6 F 13/00	5 4 0	G 0 9 C 1/00	6 6 0 A
G 0 9 C 1/00	6 6 0		6 6 0 D
		H 0 4 L 9/00	6 0 1 B
H 0 4 L 9/32			6 0 1 A

審査請求 未請求 請求項の数27 O L (全109頁) 最終頁に続く

(21) 出願番号 特願2000-362913(P2000-362913)

(22) 出願日 平成12年11月29日(2000.11.29)

(71) 出願人 000001889

三洋電機株式会社

大阪府守口市京阪本通2丁目5番5号

(71) 出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番1号

(71) 出願人 000136136

株式会社ピーエフユー

石川県河北郡宇ノ気町宇野気又98番地の2

(74) 代理人 100064746

弁理士 深見 久郎 (外3名)

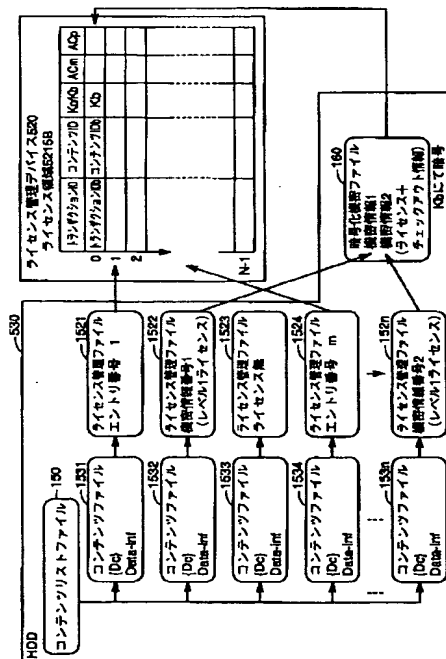
最終頁に続く

(54) 【発明の名称】 データ端末装置

(57) 【要約】

【課題】 ソフトウェアによって配信された暗号化コンテンツデータおよびライセンスを他のデータ端末装置へ移動可能なデータ端末装置を提供する。

【解決手段】 パーソナルコンピュータのハードディスク530は、コンテンツリストファイル150と暗号化機密ファイル160とを有する。ライセンス管理デバイス520は、メモリのライセンス領域5215Bにバインディング鍵Kbを格納する。暗号化機密ファイル160は、ライセンス管理デバイス520に格納されたバインディング鍵Kbによって復号および暗号化が可能である。そして、取得された暗号化コンテンツデータのライセンスは、暗号化機密ファイル160に機密情報として格納される。



## 【特許請求の範囲】

【請求項1】 コンテンツデータを暗号化した暗号化コンテンツデータおよび前記暗号化コンテンツデータを復号して元の平文を得るためのライセンスを取得し、前記暗号化コンテンツデータおよび前記ライセンスを他のデータ端末装置へ出力するデータ端末装置であって、前記暗号化コンテンツデータおよび前記ライセンスをソフトウェアによって取得するモジュール部と、前記暗号化コンテンツデータと、ライセンス管理ファイルと、暗号化機密ファイルとを記憶する記憶部と、前記暗号化機密ファイルを復号し、かつ、その復号した機密ファイルを暗号化するバイディング鍵を含むバイディングライセンスを専用領域に格納するデバイス部とを備え、

前記機密ファイルは、前記ライセンスを構成要素とする機密情報を含み、

前記ライセンス管理ファイルは、前記暗号化コンテンツファイルに対応し、かつ、前記機密ファイルに含まれる前記機密情報の管理番号を含む、データ端末装置。

【請求項2】 前記暗号化機密ファイルの初期化時、前記モジュール部は、前記バイディング鍵を含めて前記バイディングライセンスを生成し、機密情報が空な機密ファイルを生成し、その生成した機密ファイルを前記生成したバイディング鍵によって暗号化して前記暗号化機密ファイルを生成するとともに、前記生成したバイディングライセンスを前記デバイス部に与える、請求項1に記載のデータ端末装置。

【請求項3】 前記ライセンスの取得時、

前記モジュール部は、前記記憶部から読出した前記暗号化機密ファイルを前記デバイス部から取得した前記バイディング鍵によって復号し、その復号した機密ファイルに前記取得したライセンスを機密情報として書込んで前記機密ファイルを更新し、その更新した機密ファイルを前記バイディング鍵によって暗号化し、その暗号化した暗号化機密ファイルを前記記憶部に更新記録し、前記書込んだライセンスを構成要素とする機密情報の管理番号を含むライセンス管理ファイルを作成して前記記憶部に書込む、請求項1に記載のデータ端末装置。

【請求項4】 前記ライセンスの送信時、

前記モジュール部は、前記デバイス部から取得した前記バイディング鍵によって前記記憶部から読出した前記暗号化機密ファイルを復号してライセンスを取得し、その取得したライセンスを外部へ出力する、請求項1に記載のデータ端末装置。

【請求項5】 前記ライセンスの出力時、

前記モジュール部は、前記ライセンスに対応し、かつ前記記憶部に記録された前記暗号化コンテンツデータと前記ライセンスとを外部へ出力する、請求項4に記載のデータ端末装置。

【請求項6】 前記デバイス部は、前記専用領域を指定

する専用登録番号を前記モジュール部から受取り、その受取った専用登録番号によって前記バイディングライセンスを前記専用領域に格納する、請求項1に記載のデータ端末装置。

【請求項7】 前記ライセンスの出力時、前記モジュール部は、前記専用登録番号を前記デバイス部へ送信することによって前記バイディング鍵を取得する、請求項6に記載のデータ端末装置。

【請求項8】 前記ライセンスの出力時、前記モジュール部は、前記デバイス部に対する認証データを前記デバイス部へ送信し、前記デバイス部において前記認証データが認証された場合、前記バイディング鍵を取得する、請求項1から請求項7のいずれか1項に記載のデータ端末装置。

【請求項9】 前記ライセンスの出力時、前記デバイス部は、前記バイディング鍵を暗号化して出力する、請求項1から請求項8のいずれか1項に記載のデータ端末装置。

【請求項10】 前記ライセンスの出力時、前記モジュール部は、前記取得したバイディング鍵によって前記暗号化機密ファイルを復号して機密ファイルを取得し、かつ、前記記憶部から読出したライセンス管理ファイルに含まれる機密情報の管理番号に一致する機密情報を前記取得した機密ファイルから読出すことによって外部へ出力するライセンスを取得する、請求項4に記載のデータ端末装置。

【請求項11】 前記ライセンスの他のデータ端末装置への送信時、

前記モジュール部は、さらに、前記デバイス部において保持された公開暗号鍵を受取ることによって前記デバイス部はバイディングライセンスの書込みが可能であることを確認する、請求項1から請求項9のいずれか1項に記載のデータ端末装置。

【請求項12】 前記暗号化コンテンツデータの他のデータ端末装置への移動時、

前記モジュール部は、前記ライセンスの複製ができないとき、前記他のデータ端末装置へ送信したライセンスを構成要素とする機密情報を削除し、その削除した機密情報の管理番号を削除してライセンス管理ファイルを更新し、もう1つのバイディング鍵を生成し、その生成したもう1つのバイディング鍵によって機密ファイルを暗号化して前記暗号化機密ファイルを更新する、請求項10に記載のデータ端末装置。

【請求項13】 前記暗号化コンテンツデータの他のデータ端末装置への移動時、

前記デバイス部は、前記もう1つのバイディング鍵を含むもう1つのバイディングライセンスを前記モジュール部から受け取り、その受取ったもう1つのバイディングライセンスを前記専用領域に上書きして格納する、請求項11に記載のデータ端末装置。

【請求項 14】 前記ライセンスの他のデータ端末装置への送信時、

前記モジュール部は、前記他のデータ端末装置から受信した認証データを認証すると、ライセンスを他のデータ端末装置へ送信する、請求項 1 から請求項 12 のいずれか 1 項に記載のデータ端末装置。

【請求項 15】 前記モジュール部は、前記ライセンスを暗号化した上で出力する、請求項 13 に記載のデータ端末装置。

【請求項 16】 コンテンツデータを暗号化した暗号化コンテンツデータおよび前記暗号化コンテンツデータを復号して元の平文を得るためのライセンスを取得し、前記暗号化コンテンツデータおよび前記ライセンスを他のデータ端末装置へ出力するデータ端末装置であって、前記暗号化コンテンツデータおよび前記ライセンスをソフトウェアによって取得するモジュール部と、前記暗号化コンテンツデータと、ライセンス管理ファイルと、独自の暗号化を施した暗号化機密ファイルとを記憶する記憶部と、

バイディング鍵を含むバイディングライセンスを専用領域に格納するデバイス部とを備え、

前記暗号化機密ファイルを復号した機密ファイルは、前記デバイス部が格納するバイディングライセンスと同じバイディングライセンスを含み、

前記ライセンス管理ファイルは、前記暗号化コンテンツデータに対応し、かつ、前記ライセンスを構成要素とする機密情報に独自の暗号化を施した暗号化機密情報を含む、データ端末装置。

【請求項 17】 前記暗号化機密ファイルの初期化時、前記モジュール部は、前記バイディング鍵を含めて前記バイディングライセンスを生成し、その生成したバイディングライセンスを格納した機密ファイルを生成し、その生成した機密ファイルに独自の暗号化を施して前記暗号化機密ファイルを生成するとともに、前記生成したバイディングライセンスを前記デバイス部に与える、請求項 16 に記載のデータ端末装置。

【請求項 18】 前記ライセンスの取得時、前記モジュール部は、前記ライセンスに独自の暗号化を施して暗号化機密情報を生成し、その暗号化機密情報を含むライセンス管理ファイルを生成して前記記憶部に書込む、請求項 16 に記載のデータ端末装置。

【請求項 19】 前記ライセンスの送信時、前記モジュール部は、前記デバイス部から取得した前記バイディング鍵が前記暗号化機密ファイルを復号して取得したバイディング鍵に一致すると、前記記憶部から読出した前記暗号化機密情報を復号してライセンスを取得し、その取得したライセンスと前記記憶部から読出した暗号化コンテンツデータとを他のデータ端末装置へ送信する、請求項 18 に記載のデータ端末装置。

【請求項 20】 前記独自の暗号化方式は、データ端末

装置から取得可能なデータ端末装置に固有の情報に関連付けた暗号化方式である、請求項 16 に記載のデータ端末装置。

【請求項 21】 前記デバイス部は、前記専用領域を指定する専用登録番号を前記モジュール部から受取り、その受取った専用登録番号によって前記バイディングライセンスを前記専用領域に格納し、

前記モジュール部は、前記専用登録番号を含めて前記暗号化機密ファイルおよび前記ライセンス管理ファイルを生成する、請求項 16 に記載のデータ端末装置。

【請求項 22】 前記ライセンスの送信時、前記モジュール部は、前記専用登録番号を前記デバイス部へ送信することによって前記バイディング鍵を取得する、請求項 21 に記載のデータ端末装置。

【請求項 23】 前記ライセンスの他のデータ端末装置への送信時、

前記モジュール部は、前記デバイス部に対する認証データを前記デバイス部へ送信し、前記デバイス部において前記認証データが認証された場合、前記バイディング鍵を取得する、請求項 16 から請求項 23 のいずれか 1 項に記載のデータ端末装置。

【請求項 24】 前記ライセンスの他のデータ端末装置への送信時、

前記モジュール部は、前記他のデータ端末装置から受信した認証データを認証すると、ライセンスを他のデータ端末装置へ送信する、請求項 16 から請求項 23 のいずれか 1 項に記載のデータ端末装置。

【請求項 25】 前記モジュール部は、配信サーバからインターネットによって前記暗号化コンテンツデータおよび前記ライセンスを取得する、請求項 1 から請求項 24 のいずれか 1 項に記載のデータ端末装置。

【請求項 26】 記録媒体から平文のコンテンツデータを読み出す媒体駆動部をさらに備え、

前記モジュール部は、前記媒体駆動部が読出したコンテンツデータに含まれる複製可否情報に基づいてライセンスを生成し、その生成したライセンスに含まれるライセンス鍵によって前記コンテンツデータを暗号化して暗号化コンテンツデータを生成することによって前記暗号化コンテンツデータおよび前記ライセンスを取得する、請求項 1 から請求項 24 のいずれか 1 項に記載のデータ端末装置。

【請求項 27】 前記デバイス部は、さらに、配信サーバから前記暗号化コンテンツデータおよびライセンスを受信し、その受信したライセンスを保持し、

前記記憶部は、前記デバイス部によって受信された暗号化コンテンツデータを記憶する、請求項 1 から請求項 24 のいずれか 1 項に記載のデータ端末装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明は、コピーされた情

報に対する著作権保護を可能とするデータ配信システムにおいて用いられるデータ端末装置に関するものである。

【0002】

【従来の技術】近年、インターネット等の情報通信網等の進歩により、再生端末等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【0003】このような情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

【0004】したがって、このような情報通信網上において音楽データや画像データ等の著作権者の権利が存在する創作物が伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【0005】一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介して著作物データの配信を行なうことができないとすると、基本的には、著作物データの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【0006】ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタルデータを記録した記録媒体を例にとって考えて見ると、通常販売されている音楽データを記録したCD（コンパクトディスク）については、CDから光磁気ディスク（MD等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体やMD等の媒体の代金のうちの一定額を間接的に著作権者に対して著作権料として支払うことになっている。

【0007】しかも、CDからMDへデジタル信号である音楽データをコピーした場合、これらの情報がコピー劣化の殆どないデジタルデータであることに鑑み、記録可能なMDからさらに他のMDに音楽データとしてコピーすることは、著作権保護のために機器の構成上できないようになっている。

【0008】このような事情からも、音楽データや画像データをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

【0009】この場合、情報通信網を通じて公衆に送信される著作物である音楽データや画像データ等のコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されること、あるいは、複製でき

ても利用されることを防止することが必要となる。

【0010】そこで、コンテンツデータを暗号化した暗号化コンテンツデータを保持する配信サーバが、再生端末等の端末装置に装着されたメモリカードに対して端末装置を介して暗号化コンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモリカードの公開暗号鍵とその証明書を暗号化コンテンツデータの配信要求の際に配信サーバへ送信し、配信サーバが認証された証明書を受信したことを確認した上でメモリカードに対して暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンス鍵を送信する。そして、暗号化コンテンツデータやライセンス鍵を配信する際、配信サーバおよびメモリカードは、配信毎に異なるセッションキーを発生させ、その発生させたセッションキーによって公開暗号鍵の暗号化を行ない、配信サーバ、メモリカード相互間で鍵の交換を行なう。

【0011】最終的に、配信サーバは、メモリカード個々の公開暗号鍵によって暗号化され、さらにセッションキーによって暗号化したライセンスと、暗号化コンテンツデータをメモリカードに送信する。そして、メモリカードは、受信したライセンスと暗号化コンテンツデータをメモリカードに記録する。

【0012】そして、メモリカードに記録した暗号化コンテンツデータを再生するときは、メモリカードを携帯電話機に装着する。携帯電話機は、通常の電話機能の他にメモリカードからの暗号化コンテンツデータを復号し、かつ、再生して外部へ出力するための専用回路も有する。

【0013】このように、携帯電話機のユーザは、携帯電話機を用いて暗号化コンテンツデータを配信サーバから受信し、その暗号化コンテンツデータを再生することができる。

【0014】一方、インターネットを用いて暗号化コンテンツデータをパーソナルコンピュータに配信することも行なわれている。そして、パーソナルコンピュータへの暗号化コンテンツデータとライセンスを同様な方法で配信することは可能ではあるが、パーソナルコンピュータにインストールされたソフトウェアによって暗号化コンテンツデータおよびライセンスの配信が受信され、ライセンスの保護が行なわれており、受信した暗号化コンテンツデータおよびライセンスを他のパーソナルコンピュータへ移動することは著作権保護の観点から行なわれていない。

【0015】つまり、パーソナルコンピュータへ配信されたライセンスを記録したパーソナルコンピュータのCPUに個別に付与された識別番号や起動プログラムであるBIOSの識別番号などの値に関連付けた暗号処理を用いて、そのまま他のパーソナルコンピュータにコピーしても、ライセンスを取り出せず、暗号化コンテンツ復

号して再生できない管理構造を採用している。そして、この管理下においてライセンスを他のパーソナルコンピュータへ移動できるサービスを提供したとすると、記録装置上で、ライセンスを特定することはできないものの、暗号化コンテンツデータおよびライセンスを管理し、記録している全てのデータのバックアップを取っておき、提供されたサービスによって、他のパーソナルコンピュータへ暗号化コンテンツデータおよびライセンスを移動させた後に、バックアップを取った暗号化コンテンツデータおよびライセンスを管理し、記録している全てのデータをパーソナルコンピュータへ戻せば移動前の状態を再現でき、暗号化コンテンツデータおよびライセンスを複製したのと同じことになる。このような管理においてのライセンスの移動は、セキュリティホールが明らかに存在する。したがって、ソフトウェアによってパーソナルコンピュータへ配信された暗号化コンテンツデータおよびライセンスを他のパーソナルコンピュータへ移動できないことになっている。

【0016】

【発明が解決しようとする課題】しかし、パーソナルコンピュータに配信された暗号化コンテンツデータおよびライセンスをそのパーソナルコンピュータから、一切、取り出すことができないとすると、パーソナルコンピュータの破損や、バージョンアップによってCPUが変動したときは、既に受信した暗号化コンテンツデータおよびライセンスを利用することができないという問題がある。

【0017】そこで、本発明は、かかる問題を解決するためになされたものであり、その目的は、ソフトウェアによって配信された暗号化コンテンツデータおよびライセンスを他のデータ端末装置へ移動可能なデータ端末装置を提供することである。

【0018】

【課題を解決するための手段および発明の効果】この発明によるデータ端末装置は、コンテンツデータを暗号化した暗号化コンテンツデータおよび暗号化コンテンツデータを復号して元の平文を得るためのライセンスを取得し、暗号化コンテンツデータおよびライセンスを他のデータ端末装置へ出力するデータ端末装置であって、暗号化コンテンツデータおよびライセンスをソフトウェアによって取得するモジュール部と、暗号化コンテンツデータと、ライセンス管理ファイルと、暗号化機密ファイルとを記憶する記憶部と、暗号化機密ファイルを復号し、かつ、その復号した機密ファイルを暗号化するバイディング鍵を含むバイディングライセンスを専用領域に格納するデバイス部とを備え、機密ファイルは、ライセンスを構成要素とする機密情報を含み、ライセンス管理ファイルは、暗号化コンテンツファイルに対応し、かつ、機密ファイルに含まれる機密情報の管理番号を含む。

【0019】この発明によるデータ端末装置においては、モジュール部は、ソフトウェアによって暗号化コンテンツデータおよびライセンスを取得し、デバイス部から取出したバイディング鍵によって暗号化機密ファイルを復号し、取得したライセンスを復号した機密ファイルに書込み、バイディング鍵によって機密ファイルを暗号化して暗号化機密ファイルを生成する。つまり、モジュール部は、デバイス部においてハードウェアによって保持されるバイディング鍵を介して暗号化機密ファイルを開閉して取得したライセンスを管理する。

【0020】したがって、この発明によれば、ソフトウェアによって取得された暗号化コンテンツデータを復号して再生するためのライセンスは、ハードウェアに保持されたバイディング鍵によって管理されるため、取得した暗号化コンテンツデータおよびライセンスを他のデータ端末装置へ移動できる。

【0021】好ましくは、暗号化機密ファイルの初期化時、データ端末装置のモジュール部は、バイディング鍵を含めてバイディングライセンスを生成し、機密情報が空な機密ファイルを生成し、その生成した機密ファイルを生成したバイディング鍵によって暗号化して暗号化機密ファイルを生成するとともに、生成したバイディングライセンスをデバイス部に与える。

【0022】暗号化機密ファイルの初期化時、モジュール部は、バイディング鍵を含むバイディングライセンスと空な機密ファイルとを生成し、機密ファイルをバイディング鍵によって暗号化を行なって暗号化機密ファイルを生成するとともにバイディングライセンスをデバイス部に保持する。

【0023】したがって、この発明によれば、ソフトウェアによって取得した暗号化コンテンツデータのライセンスを格納する機密ファイルをソフト的に作成し、その作成した機密ファイルを管理するためのバイディングライセンスをハード的に管理できる。

【0024】好ましくは、ライセンスの取得時、データ端末装置のモジュール部は、記憶部から読出した暗号化機密ファイルをデバイス部から取得したバイディング鍵によって復号し、その復号した機密ファイルに取得したライセンスを機密情報として書込んで機密ファイルを更新し、その更新した機密ファイルをバイディング鍵によって暗号化し、その暗号化した暗号化機密ファイルを記憶部に更新記録し、書込んだライセンスを構成要素とする機密情報の管理番号を含むライセンス管理ファイルを作成して記憶部に書込む。

【0025】デバイス部から取得したバイディング鍵によって暗号化機密ファイルを開閉して取得したライセンスを機密ファイルに書込む。そして、その書込んだライセンスを構成要素とする機密情報の管理番号を含めてライセンス管理ファイルを作成する。

【0026】したがって、この発明によれば、ソフト的

に取得した暗号化コンテンツデータのライセンスを管理番号によって管理できる。

【0027】好ましくは、ライセンスの送信時、データ端末装置のモジュール部は、デバイス部から取得したバイディング鍵によって記憶部から読出した暗号化機密ファイルを復号してライセンスを取得し、その取得したライセンスを外部へ出力する。

【0028】モジュール部は、デバイス部から取得したバイディング鍵によって暗号化機密ファイルを復号してライセンスを取得し、その取得したライセンスを外部へ出力する。

【0029】したがって、この発明によれば、ソフト的に取得した暗号化コンテンツデータのライセンスをハード的に取得した暗号化コンテンツデータのライセンスと同じように他の装置へ移動できる。

【0030】好ましくは、データ端末装置のモジュール部は、ライセンスの出力時、ライセンスに対応し、かつ記憶部に記録された暗号化コンテンツデータとライセンスとを外部へ出力する。

【0031】ライセンスの外部への出力時、機密ファイルから取出したライセンスに対応する暗号化コンテンツデータを記憶部から読出し、暗号化コンテンツデータとライセンスとを外部へ出力する。

【0032】したがって、この発明によれば、暗号化コンテンツデータおよびライセンスをソフト的に読出して他の装置へ暗号化コンテンツデータおよびライセンスを移動できる。

【0033】好ましくは、データ端末装置のデバイス部は、専用領域を指定する専用登録番号をモジュール部から受取り、その受取った専用登録番号によってバイディングライセンスを専用領域に格納する。

【0034】デバイス部は、専用登録番号を介して暗号化機密ファイルを開閉するためのバイディングライセンスを専用領域に格納する。

【0035】したがって、この発明によれば、専用登録番号によってバイディングライセンスと暗号化コンテンツデータのライセンスとを対応付けることができる。

【0036】好ましくは、ライセンスの出力時、データ端末装置のモジュール部は、専用登録番号をデバイス部へ送信することによってバイディング鍵を取得する。

【0037】モジュール部は、専用登録番号を介して、記憶部から読出したいライセンスが格納された機密ファイルを開けるためのバイディング鍵を取得する。

【0038】したがって、この発明によれば、専用登録番号によってバイディング鍵を正確に取得できる。

【0039】好ましくは、ライセンスの出力時、データ端末装置のモジュール部は、デバイス部に対する認証データをデバイス部へ送信し、デバイス部において認証データが認証された場合、バイディング鍵を取得する。

【0040】認証されたモジュール部のみにバイディ

ング鍵が与えられる。したがって、この発明によれば、不正なバイディング鍵の流出を防止できる。

【0041】好ましくは、ライセンスの出力時、データ端末装置のデバイス部は、バイディング鍵を暗号化して出力する。

【0042】デバイス部は、ライセンスを管理するためのバイディング鍵を暗号化して出力する。

【0043】したがって、この発明によれば、ライセンスを他の装置へ移動するとき、移動先でライセンスを管理するバイディング鍵を不正に取得されにくくできる。

【0044】好ましくは、ライセンスの出力時、データ端末装置のモジュール部は、取得したバイディング鍵によって暗号化機密ファイルを復号して機密ファイルを取得し、かつ、記憶部から読出したライセンス管理ファイルに含まれる機密情報の管理番号に一致する機密情報取得した機密ファイルから読出すことによって外部へ出力するライセンスを取得する。

【0045】モジュール部は、デバイス部からバイディング鍵を取得して暗号化機密ファイルを復号し、その復号した機密ファイルに含まれる機密情報から管理番号に一致する機密情報を取得して外部へ出力しようとするライセンスを取得する。

【0046】したがって、この発明によれば、管理番号を介して正確にライセンスを取得できる。

【0047】好ましくは、ライセンスの他のデータ端末装置への送信時、データ端末装置のモジュール部は、さらに、デバイス部において保持された公開暗号鍵を受取ることによってデバイス部はバイディングライセンスの書込みが可能であることを確認する。

【0048】モジュール部は、ライセンスの他の装置への送信時、デバイス部がバイディングライセンスの書込みが可能か否かをデバイス部から公開暗号鍵を受取ることによって確認する。

【0049】したがって、この発明によれば、暗号化コンテンツデータのライセンスを移動した際、デバイス部に格納されたバイディングライセンスを書換えることによってライセンスを移動したことを認識可能である。

【0050】好ましくは、暗号化コンテンツデータの他のデータ端末装置への移動時、データ端末装置のモジュール部は、ライセンスの複製ができないとき、他のデータ端末装置へ送信したライセンスを構成要素とする機密情報を削除し、その削除した機密情報の管理番号を削除してライセンス管理ファイルを更新し、もう1つのバイディング鍵を生成し、その生成したもう1つのバイディング鍵によって機密ファイルを暗号化して暗号化機密ファイルを更新する。

【0051】移動したライセンスの複製が禁止されているとき、モジュール部は、移動したライセンスを削除するとともに、別のバイディング鍵を生成して暗号化機



密ファイルを更新する。

【0052】したがって、この発明によれば、ライセンスが不正に複製されるのを防止できる。

【0053】好ましくは、暗号化コンテンツデータの他のデータ端末装置への移動時、データ端末装置のデバイス部は、もう1つのバイディング鍵を含むもう1つのバイディングライセンスをモジュール部から受け取り、その受取ったもう1つのバイディングライセンスを専用領域に上書きして格納する。

【0054】別のバイディング鍵が生成されたとき、デバイス部においてバイディングライセンスの書換えが行なわれる。

【0055】したがって、この発明によれば、最新のバイディングライセンスによって暗号化コンテンツデータを再生するためのライセンスを管理できる。

【0056】好ましくは、ライセンスの他のデータ端末装置への送信時、データ端末装置のモジュール部は、他のデータ端末装置から受信した認証データを認証すると、ライセンスを他のデータ端末装置へ送信する。

【0057】モジュール部は、暗号化コンテンツデータのライセンスを移動しようとするデータ端末装置が正規の端末装置であることを確認してから暗号化コンテンツデータのライセンスを送信する。

【0058】したがって、この発明によれば、正規なデータ端末装置間で暗号化コンテンツデータのライセンスを移動でき、暗号化コンテンツデータを十分に保護できる。

【0059】好ましくは、データ端末装置のモジュール部は、ライセンスを暗号化した上で出力する。

【0060】モジュール部は、ライセンスを暗号化した上で他のデータ端末装置へ移動する。

【0061】したがって、この発明によれば、ライセンスの移動時に、そのライセンスを不正に取得されにくい。

【0062】また、この発明によるデータ端末装置は、コンテンツデータを暗号化した暗号化コンテンツデータおよび暗号化コンテンツデータを復号して元の平文を得るためのライセンスを取得し、暗号化コンテンツデータおよびライセンスを他のデータ端末装置へ出力するデータ端末装置であって、暗号化コンテンツデータおよびライセンスをソフトウェアによって取得するモジュール部と、暗号化コンテンツデータと、ライセンス管理ファイルと、独自の暗号化を施した暗号化機密ファイルとを記憶する記憶部と、バイディング鍵を含むバイディングライセンスを専用領域に格納するデバイス部とを備え、暗号化機密ファイルを復号した機密ファイルは、デバイス部が格納するバイディングライセンスと同じバイディングライセンスを含み、ライセンス管理ファイルは、暗号化コンテンツデータに対応し、かつ、ライセンスを構成要素とする機密情報に独自の暗号化を施した

暗号化機密情報を含む。

【0063】この発明によるデータ端末装置においては、モジュール部は、ソフトウェアによって暗号化コンテンツデータおよびライセンスを取得し、その取得したライセンスに独自の暗号化を施して暗号化機密情報を生成し、その生成した暗号化機密情報を含むライセンス管理ファイルを作成して記憶部に書込む。また、ライセンスを管理するバイディングライセンスは機密ファイルに格納される。

【0064】したがって、この発明によれば、ライセンスを管理するためのバイディング鍵はハードウェアによって保持されるため、ソフトウェアによって取得された暗号化コンテンツデータを復号して再生するためのライセンスを他のデータ端末装置へ移動できる。

【0065】好ましくは、暗号化機密ファイルの初期化時、データ端末装置のモジュール部は、バイディング鍵を含めてバイディングライセンスを生成し、その生成したバイディングライセンスを格納した機密ファイルを生成し、その生成した機密ファイルに独自の暗号化を施して暗号化機密ファイルを生成するとともに、生成したバイディングライセンスをデバイス部に与える。

【0066】モジュール部は、暗号化機密ファイルの初期化時、バイディング鍵を含むバイディングライセンスと空な機密ファイルとを生成し、機密ファイルに生成したバイディングライセンスを書込んで独自の暗号化を行なって暗号化機密ファイルを生成するとともにバイディングライセンスをデバイス部の専用領域に保持する。

【0067】したがって、この発明によれば、ライセンスを管理するためのバイディング鍵はハードウェアによって保持されるため、ソフトウェアによって取得された暗号化コンテンツデータを復号して再生するためのライセンスを他のデータ端末装置へ移動できる。

【0068】好ましくは、ライセンスの取得時、データ端末装置のモジュール部は、ライセンスに独自の暗号化を施して暗号化機密情報を生成し、その暗号化機密情報を含むライセンス管理ファイルを生成して記憶部に書込む。

【0069】モジュール部は、取得したライセンスに独自の暗号化を施して記憶部で管理する。

【0070】したがって、この発明によれば、ライセンスを独自の暗号化方式によって管理できる。

【0071】好ましくは、ライセンスの送信時、データ端末装置のモジュール部は、デバイス部から取得したバイディング鍵が暗号化機密ファイルを復号して取得したバイディング鍵に一致すると、記憶部から読出した暗号化機密情報を復号してライセンスを取得し、その取得したライセンスと記憶部から読出した暗号化コンテンツデータとを他のデータ端末装置へ送信する。

【0072】モジュール部は、デバイス部に格納された

バイディング鍵と記憶部に格納されたバイディング鍵とが一致する場合に限り、ライセンスを取得する。

【0073】したがって、ハード的に管理されたバイディング鍵と同じバイディング鍵を有するモジュール部だけがライセンスを取得できる。

【0074】好ましくは、独自の暗号化方式は、データ端末装置から取得可能なデータ端末装置に固有の情報に関連付けた暗号化方式である。

【0075】モジュール部は、データ端末装置に固有な情報、たとえば、CPUのバージョン番号等に基づいた暗号化方式によってライセンスを暗号化する。

【0076】したがって、この発明によれば、暗号化されたライセンスが他の装置へ不正に流出されても、そのライセンスが不正に取得されない。

【0077】好ましくは、データ端末装置のデバイス部は、専用領域を指定する専用登録番号をモジュール部から受取り、その受取った専用登録番号によってバイディングライセンスを専用領域に格納し、モジュール部は、専用登録番号を含めて暗号化機密ファイルおよびライセンス管理ファイルを生成する。

【0078】デバイス部は、モジュール部によって生成された専用登録番号によってバイディングライセンスをハード的に管理し、モジュール部は、生成した専用登録番号と取得したライセンスとを独自に暗号化してソフト的に管理する。

【0079】したがって、この発明によれば、モジュール部は、専用登録番号を介してデバイス部に保持されたバイディング鍵を取得し、暗号化機密ファイルから読出したバイディング鍵とデバイス部から取得したバイディング鍵との一致を正確に判別できる。

【0080】好ましくは、ライセンスの送信時、データ端末装置のモジュール部は、専用登録番号をデバイス部へ送信することによってバイディング鍵を取得する。

【0081】モジュール部は、専用登録番号をデバイス部へ送信し、デバイス部は受信した専用登録番号によって指定された専用領域からバイディング鍵を取出して出力する。

【0082】したがって、この発明によれば、専用登録番号によってバイディング鍵を正確に取得できる。

【0083】好ましくは、ライセンスの他のデータ端末装置への送信時、データ端末装置のモジュール部は、デバイス部に対する認証データをデバイス部へ送信し、デバイス部において認証データが認証された場合、バイディング鍵を取得する。

【0084】モジュール部のデバイス部に対する正当性が確認された場合だけ、モジュール部がバイディング鍵を取得する。

【0085】したがって、この発明によれば、バイディング鍵の不正な取得を防止でき、その結果、ライセンスが他の端末装置へ不正に移動されることを防止でき

る。

【0086】好ましくは、ライセンスの他のデータ端末装置への送信時、データ端末装置のモジュール部は、他のデータ端末装置から受信した認証データを認証すると、ライセンスを他のデータ端末装置へ送信する。

【0087】暗号化コンテンツデータおよびライセンスを移動しようとするデータ端末装置が正規であることが確認されると、モジュール部は暗号化コンテンツデータおよびライセンスを他のデータ端末装置へ送信する。

【0088】したがって、この発明によれば、正規のデータ端末装置間でのみ、暗号化コンテンツデータおよびライセンスの移動が可能である。

【0089】好ましくは、データ端末装置のモジュール部は、配信サーバからインターネットによって暗号化コンテンツデータおよびライセンスを取得する。

【0090】したがって、この発明によれば、各種のコンテンツデータを取得し、かつ、他の端末装置へ取得したコンテンツデータを移動できる。

【0091】好ましくは、データ端末装置は、記録媒体から平文のコンテンツデータを読出す媒体駆動部をさらに備え、モジュール部は、媒体駆動部が読出したコンテンツデータに含まれる複製可否情報に基づいてライセンスを生成し、その生成したライセンスに含まれるライセンス鍵によってコンテンツデータを暗号化して暗号化コンテンツデータを生成することによって暗号化コンテンツデータおよびライセンスを取得する。

【0092】データ端末装置は、リッピングによって暗号化コンテンツデータおよびライセンスを取得する。

【0093】したがって、この発明によれば、通信手段以外の手段で頒布されるコンテンツデータも取得し、他のデータ端末装置へ移動できる。

【0094】好ましくは、データ端末装置のデバイス部は、さらに、配信サーバから暗号化コンテンツデータおよびライセンスを受信し、その受信したライセンスを保持し、記憶部は、デバイス部によって受信された暗号化コンテンツデータを記憶する。

【0095】デバイス部は、バイディングライセンスを保持するとともに、配信サーバから暗号化コンテンツデータおよびライセンスを受信し、その受信したライセンスをバイディングライセンスとともに保持する。

【0096】したがって、この発明によれば、ハードウェアによって取得したライセンスとソフトウェアによって取得したライセンスとを殆ど同じセキュリティレベルで管理できる。

【0097】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【0098】【実施の形態1】図1は、本発明によるデータ端末装置（パーソナルコンピュータ）が暗号化コン

テンツデータを取得するとともに、その取得した暗号化コンテンツデータを他のデータ端末装置（パーソナルコンピュータ）へ移動するデータ配信システムの全体構成を概念的に説明するための概略図である。

【0099】なお、以下ではインターネットを介してデジタル音楽データを各パーソナルコンピュータのユーザに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物としてのコンテンツデータ、たとえば画像データ、動画像データ等を配信する場合においても適用することが可能なものである。

【0100】図1を参照して、パーソナルコンピュータ50は、モデム40およびインターネット網30を介して、各パーソナルコンピュータのユーザからの配信要求（配信リクエスト）を配信サーバ10に送信する。著作権の存在する音楽データを管理する配信サーバ10は、データ配信を求めてアクセスして来たパーソナルコンピュータのユーザが所有するパーソナルコンピュータ50が正当な認証データを持つか否か、すなわち、正規のパーソナルコンピュータは充分なセキュリティレベルを備えたコンテンツ保護を行っているか否かの認証処理を行ない、正当なコンテンツ保護を行っているパーソナルコンピュータに対して所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化した上で、このような暗号化コンテンツデータおよび暗号化コンテンツデータを再生するために必要な情報としてのライセンスをパーソナルコンピュータ50に配信する。

【0101】この場合、パーソナルコンピュータ50は、モデム40およびインターネット網30を介して異なるセキュリティレベルによって暗号化コンテンツデータおよびライセンスを配信サーバ10から受信して、管理することができる。すなわち、パーソナルコンピュータ50は、ハード的にコンテンツ点津保護を実現するライセンス管理デバイスと、ソフト的にコンテンツ保護を実現するライセンス管理モジュールとを内蔵している。ライセンス管理デバイスは、アプリケーションソフトの助けを得て、配信サーバ10からインターネット網30等を介して暗号化コンテンツデータおよびライセンスを受信する。このライセンス管理デバイスは、暗号化コンテンツデータを再生するためのライセンスを受信するための暗号通信路を、直接、配信サーバとの間で確立し、受信したライセンスをハード的に保持するものであり、セキュリティレベルが高いものである。また、ライセンス管理モジュールも、同様に、所定の手順に従った暗号通信路を配信サーバとの間で確立し、ライセンスを受信し、暗号化して保護した上で、ハードディスク（HDDと言う）にライセンスを記録する。ライセンス管理デバイスよりも低いセキュリティレベルで暗号化コンテンツデータおよびライセンスを受信し、管理するものであ

る。いずれの場合においても、暗号化コンテンツデータはそのままHDDに記録される。ライセンス管理デバイスおよびライセンス管理モジュールについては、後に詳細に説明する。

【0102】以後、セキュリティレベルおよびライセンスを区別するためにメモリカード110あるいはライセンス管理デバイスなどのハードウェアによって機密性を保つセキュリティレベルをレベル2と呼び、レベル2のセキュリティを要求して配信サーバから送信されるライセンスをレベル2ライセンスと呼ぶこととする。同様に、ライセンス管理モジュールのようなソフトウェアによって機密性を保つセキュリティレベルをレベル1と呼び、レベル1のセキュリティレベルを要求して配信サーバから送信されるライセンスをレベル1ライセンスと呼ぶこととする。

【0103】さらに、図1においては、パーソナルコンピュータ50は、ライセンス管理モジュールを使って音楽データを記録した音楽CD（Compact Disk）60から取得した音楽データから、個人使用に限定したローカル使用に限定された暗号化コンテンツデータと、暗号化コンテンツデータを再生するためのライセンスとを生成することができる。この処理をリッピングと呼び、音楽CDから暗号化コンテンツデータとライセンスとを取得する行為に相当する。リッピングによるローカル使用のライセンスは、その性格上、セキュリティレベルは決して高くないので、リッピングが如何なる手段でなされようともレベル1ライセンスとして扱われるものとする。リッピングの詳細については後述する。

【0104】またさらに、パーソナルコンピュータ50は、USB（Universal Serial Bus）ケーブル70によって再生端末100と接続し、配信サーバ10から受信した暗号化コンテンツデータおよびライセンスを再生端末100に装着されたメモリカード110に送信することが可能である。

【0105】またさらに、パーソナルコンピュータ50は、受信した暗号化コンテンツデータおよびライセンスを通信ケーブル90を介して、パーソナルコンピュータ80へ送信する。

【0106】したがって、図1に示すデータ配信システムにおいては、パーソナルコンピュータ50は、モデム40およびインターネット網30を介して配信サーバ10から暗号化コンテンツデータとライセンスとを受信するとともに、音楽CDから暗号化コンテンツデータとライセンスとを取得する。また、再生端末100に装着されたメモリカード110は、パーソナルコンピュータ50が配信サーバ10または音楽CD60から取得した暗号化コンテンツデータおよびライセンスを受信する。再生端末100のユーザは、パーソナルコンピュータ50を介することによって音楽CDから暗号化コンテンツデータおよびライセンスを取得することが可能となる。

【0107】図1においては、たとえば携帯電話ユーザの再生端末100には、着脱可能なメモリカード110が装着される構成となっている。メモリカード110は、再生端末100により受信された暗号化コンテンツデータを受取り、上記配信にあたって行なわれた暗号化を復号した上で、再生端末100中の音楽再生部(図示せず)に与える。

【0108】さらに、たとえば携帯電話ユーザは、再生端末100に接続したヘッドホン130等を介してこのようなコンテンツデータを「再生」して、聴取することが可能である。

【0109】また、図1においては、パーソナルコンピュータ50は、ライセンス管理モジュールを使って、ライセンス管理モジュールが直接管理するレベル1ライセンスを持つ暗号化コンテンツデータに限り、ライセンス管理モジュールと密接な連携を取る音楽再生プログラムを用いて再生する機能を備えることができる。レベル2ライセンスを持つ暗号化コンテンツデータの再生は、再生端末と同様な構成を持つハードウェアによって機密性を持つコンテンツ再生回路をパーソナルコンピュータに備えれば可能となる。パーソナルコンピュータにおける再生についての詳細な説明は、本出願における説明を簡略化するために省略する。

【0110】このような構成とすることで、十分なセキュリティレベルのコンテンツ保護機能をもつ、正規なライセンス管理デバイスあるいはライセンス管理モジュールを備えたパーソナルコンピュータでない、配信サーバ10からコンテンツデータの配信を受信し、パーソナルコンピュータ80や再生端末100へ暗号化コンテンツデータを送信することが困難な構成となる。

【0111】しかも、配信サーバ10において、たとえば1曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、パーソナルコンピュータのユーザがコンテンツデータを受信(ダウンロード)するたびに発生する著作権料を、インターネット網の使用料とともに徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【0112】なお、図1において、再生端末100は、配信サーバ10と直接通信する機能を有しない再生端末を想定している。

【0113】図1に示したような構成においては、暗号化して配信されるコンテンツデータをパーソナルコンピュータのユーザ側で再生可能とするためにシステム上必要とされるのは、第1には、通信における暗号鍵を配信するための方式であり、さらに第2には、配信したいコンテンツデータを暗号化する方式そのものであり、さらに、第3には、このように配信されたコンテンツデータの無断コピーを防止するためのコンテンツデータ保護を実現する構成である。

【0114】本発明の実施の形態においては、特に、配

信、移動、チェックアウト、チェックイン、および再生の各セッションの発生時において、これらのコンテンツデータの移動先に対する認証およびチェック機能を充実させ、非認証もしくは復号鍵の破られた記録装置およびデータ再生端末(コンテンツを再生できるデータ再生端末を再生端末またはパーソナルコンピュータとも言う。以下同じ)に対するコンテンツデータの出力を防止することによってコンテンツデータの著作権保護を強化する構成を説明する。

10 【0115】なお、以下の説明においては、配信サーバ10から、各パーソナルコンピュータ等にコンテンツデータを伝送する処理を「配信」と称することとする。

【0116】図2は、図1に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する図である。

【0117】まず、配信サーバ10より配信されるデータについて説明する。Dcは、音楽データ等のコンテンツデータである。コンテンツデータDcは、ライセンス鍵Kcで復号可能な暗号化が施される。ライセンス鍵Kcによって復号可能な暗号化が施された暗号化コンテンツデータ{Dc}Kcがこの形式で配信サーバ10よりパーソナルコンピュータのユーザに配布される。

【0118】なお、以下においては、{Y}Xという表記は、データYを、復号鍵Xにより復号可能な暗号化を施したことを示すものとする。

【0119】さらに、配信サーバ10からは、暗号化コンテンツデータとともに、コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報としての付加情報Dc-infが配布される。また、ライセンスとして、ライセンス鍵Kc、配信サーバ10からのライセンス鍵等の配信を特定するための管理コードであるトランザクションIDが配信サーバ10とパーソナルコンピュータ50との間でやり取りされる。また、配信によらないライセンス、すなわち、個人使用を目的としたローカルでの使用のライセンスを特定するためにもトランザクションIDは使用される。配信によるものと、ローカル使用のものを区別するために、トランザクションIDの先頭は“0”で始まるものがローカル使用のトランザクションIDであり、“0”以外から始まるものを配信によるトランザクションIDであるとす。さら

40 に、ライセンスとしては、コンテンツデータDcを識別するためのコードであるコンテンツID、利用者側からの指定によって決定されるライセンス数や機能限定等の情報を含んだライセンス購入条件ACに基づいて生成される、記録装置(メモリカード、またはライセンス管理デバイス)におけるライセンスのアクセスに対する制限に関する情報であるアクセス制御情報ACmおよびデータ再生端末における制御情報である再生制御情報ACp等が存在する。具体的には、アクセス制限情報ACmはメモリカード、ライセンス管理モジュールおよびライセ

ンス管理モジュールからのライセンスまたはライセンス鍵を外部に出力に対するにあった手の制御情報であり、再生可能回数（再生のためにライセンス鍵を出力する数）、ライセンスの移動・複製に関する制限情報およびライセンスのセキュリティレベルなどがある。再生制御情報ACpは、再生するためにコンテンツ再生回路がライセンス鍵を受取った後に、再生を制限する情報であり、再生期限、再生速度変更制限、再生範囲指定（部分ライセンス）などがある。

【0120】本発明の実施の形態においては、簡単化のためアクセス制限情報ACmは再生回数の制限を行なう制御情報である再生回数（0：再生不可、1～254：再生可能回数、255：制限無し）、ライセンスの移動および複製を制限する移動複製フラグ（0：移動複製禁止・1：移動のみ可・2：移動複製可）、セキュリティレベル「1：レベル1、2：レベル2」の3項目とし、再生制御情報ACpは再生可能な期限を規定する制御情報である再生期限「UTCtimeコード」のみを制限するものとする。ゆえに、以降では、再生制御情報ACpを再生期限ACpとも称する。

【0121】さらに、以後、トランザクションIDとコンテンツIDとを併せてライセンスIDと総称し、ライセンス鍵KcとライセンスIDとアクセス制限情報ACmと再生期限ACpとを併せて、ライセンスと総称することとする。

【0122】本発明の実施の形態においては、記録装置（メモリカード、ライセンス管理デバイスおよびライセンス管理モジュール）やコンテンツデータを再生する再生端末のクラスごとに、コンテンツデータの配信、および再生を禁止することができるように禁止クラスリストCRL（Class Revocation List）の運用を行なう。以下では、必要に応じて記号CRLによって禁止クラスリスト内のデータを表わすこともある。

【0123】禁止クラスリスト関連情報には、ライセンスの配信、移動、チェックアウト、および再生が禁止される再生端末、メモリカード、ライセンス管理モジュール、およびライセンス管理デバイスのクラスをリストアップした禁止クラスリストデータCRLが含まれる。コンテンツデータ保護に関わるライセンスの管理・蓄積およびライセンスを受けて再生を行なう全ての機器およびプログラムがリストアップの対象となる。

【0124】禁止クラスリストデータCRLは、配信サーバ10内で管理されるとともに、メモリカードや、ライセンス管理モジュールによってパーソナルコンピュータ50内のハードディスク（HDD）またはライセンス管理デバイス内にも記録保持される。このような禁止クラスリストは、随時バージョンアップしデータを更新していく必要があるが、データの変更については、基本的には暗号化コンテンツデータおよび／またはライセンス

鍵等のライセンスを配信する際に、パーソナルコンピュータ（ライセンス管理デバイスまたはライセンス管理モジュール）から受取った禁止クラスリストの更新日時を判断し、更新されていないと判断されたとき、更新された禁止クラスリストをパーソナルコンピュータに配信する。また、ライセンス管理モジュール、ライセンス管理デバイス、および再生端末100の間でも禁止クラスリストはやり取りされ、そのデータ変更も上述したのと同じである。さらに、禁止クラスリストの変更については、変更点のみを反映した差分データCRLを配信サーバ10側より発生して、これに応じてメモリカード、ハードディスク、およびライセンス管理デバイス内の禁止クラスリストCRLに追加する構成とすることも可能である。また、禁止クラスリストの更新日時CRLdateについては、メモリカード、ハードディスク、およびライセンス管理デバイス内に記録された禁止クラスリストCRL内に記録されていて、これを配信サーバ10側で確認することによってバージョン管理を実行する。差分データCRL更新日時CRLdateも含まれる。

【0125】このように、禁止クラスリストCRLを、配信サーバのみならずメモリカードまたはパーソナルコンピュータ内においても保持運用することによって、クラス固有すなわち、再生端末およびメモリカードまたはパーソナルコンピュータ（ライセンス管理デバイスまたはライセンス管理モジュール）の種類に固有の復号鍵が破られた、再生端末およびメモリカードまたはパーソナルコンピュータへのライセンス鍵の供給を禁止する。このため、再生端末ではコンテンツデータの再生が、メモリカード、ライセンス管理モジュール、およびライセンス管理デバイスでは新たなライセンスを受信することができなくなる。

【0126】このように、メモリカードまたはライセンス管理デバイス内の、あるいはライセンス管理モジュールが管理するHDD内の禁止クラスリストCRLは配信時に逐次データを更新する構成とする。また、メモリカード、ライセンス管理モジュール、およびライセンス管理デバイスにおける禁止クラスリストCRLの管理は、上位レベルとは独立にメモリカード、ライセンス管理デバイス、およびライセンス管理モジュールによって制御されるハードディスクでタンパーレジスタントモジュール（Tamper Resistant Module）に記録する。メモリカードまたはライセンス管理デバイス内では、ライセンスと同様に、ハード的に機密性を保証する高いレベルのタンパレジスタントモジュールによって記録され、ライセンス管理モジュールが管理するHDD内に記録された禁止クラスリストCRLの管理は、暗号処理によって少なくとも改ざん防止処置が行われてパーソナルコンピュータのHDD等に記録される。言い換えれば、ソフトウェアによってその機密性が保証された低いレベルのタンパーレジスタントモジュールによって

記録される。いずれにしても、ファイルシステムやアプリケーションプログラム等によって上位レベルから禁止クラスリストデータCRLを改ざんすることが不可能な構成とする。この結果、データに関する著作権保護をより強固なものとすることができる。

【0127】図3は、図1に示すデータ配信システムにおいて使用される認証のためのデータ、情報等の特性を説明する図である。

【0128】再生端末、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールには固有の公開暗号鍵K P p yおよびK P m wがそれぞれ設けられ、公開暗号鍵K P p yおよびK P m wは再生端末に固有の秘密復号鍵K p yおよびメモリカード、ライセンス管理デバイス、およびライセンス管理モジュールに固有の秘密復号鍵K m wによってそれぞれ復号可能である。これら公開暗号鍵および秘密復号鍵は、再生端末、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールの種類ごとに異なる値を持つ。これらの公開暗号鍵および秘密復号鍵を総称してクラス鍵と称し、これらの公開暗号鍵をクラス公開暗号鍵、秘密復号鍵をクラス秘密復号鍵、クラス鍵を共有する単位をクラスと称する。クラスは、製造会社や製品の種類、製造時のロット等によって異なる。

【0129】また、コンテンツ再生デバイス（再生端末）のクラス証明書としてC p yが設けられ、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールのクラス証明書としてC m wが設けられる。

【0130】これらのクラス証明書は、コンテンツ再生デバイス、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールのクラスごとに異なる情報を有する。タンパーレジスタントモジュールが破られたり、クラス鍵による暗号が破られた、すなわち、クラス秘密復号鍵が取得されたクラス鍵に対しては、禁止クラスリストにリストアップされてライセンスの送信の禁止対象となる。

【0131】これらのコンテンツ再生デバイス、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールに固有のクラス公開暗号鍵およびクラス証明書は、認証データ {K P p y / C p y} K P a の形式または認証データ {K P m w / C m w} K P a の形式で、出荷時にデータ再生デバイス（再生端末）、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールにそれぞれ記録される。後ほど詳細に説明するが、K P a は配信システム全体で共通の公開認証鍵である。

【0132】さらに、メモリカード110、ライセンス管理デバイス、およびライセンス管理モジュール内のデータ処理を管理するための鍵として、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールという媒体または管理ソフトウェアごとに設定される

公開暗号鍵K P m c xと、公開暗号鍵K P m c xで暗号化されたデータを復号することが可能なそれぞれに固有の秘密復号鍵K m c xが存在する。このメモリカード毎に子別な公開暗号鍵および秘密復号鍵を総称して個別鍵と称し、公開暗号鍵K P m c xを個別公開暗号鍵、秘密復号鍵K m c xを個別秘密復号鍵と称する。

【0133】メモリカード外とメモリカード間でのデータ授受、またはライセンス管理デバイス外とライセンス管理デバイス間でのデータ授受、またはライセンス管理モジュール外とライセンス管理モジュール間でのデータ授受における秘密保持のための暗号鍵として、コンテンツデータの配信、および再生が行なわれるごとに配信サーバ10、再生端末100、メモリカード110、ライセンス管理デバイス、ライセンス管理モジュールにおいて生成される共通鍵K s 1 ~ K s 3 が用いられる。

【0134】ここで、共通鍵K s 1 ~ K s 3 は、配信サーバ、再生端末もしくはメモリカードもしくはライセンス管理デバイスもしくはライセンス管理モジュール間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵K s 1 ~ K s 3 を「セッションキー」とも呼ぶこととする。

【0135】これらのセッションキーK s 1 ~ K s 3 は、各セッションごとに固有の値を有することにより、配信サーバ、再生端末、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールによって管理される。具体的には、セッションキーK s 1 は、配信サーバによって配信セッションごとに発生される。セッションキーK s 2 は、メモリカード、ライセンス管理デバイス、ライセンス管理モジュールによって配信セッションおよび再生セッションごとに発生し、セッションキーK s 3 は、再生端末において再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行したうえでライセンス鍵等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

【0136】図4は、ソフトウェア（ライセンス管理モジュール）によって取得した暗号化コンテンツデータおよびライセンスを他のパーソナルコンピュータへ移動可能とするためにライセンス管理デバイスに関連付けて暗号化し管理するために必要なバイディングライセンスと、ソフトウェアによって取得した暗号化コンテンツデータおよびライセンスをメモリカード110へ貸出すチェックアウトセッションにおけるチェックアウト管理情報とを示したものである。

【0137】バイディングライセンスは、暗号化コンテンツデータを再生するためのレベル1ライセンスと、ライセンスのチェックアウトに関する情報を暗号化し

て、ソフトタンバレジスタントモジュールを実現するための共通鍵であるバイディング鍵と、バイディングライセンスに対する制御情報であるACmb、ACpbと、バイディングライセンス用のトランザクションIDであるトランザクションIDbと、バイディングID用のダミーであるコンテンツIDbと、トランザクションIDbとコンテンツIDbとの総称であるバイディングIDとから成る。すなわち、ライセンス管理デバイスにライセンスとして記録することを前提としているため、ライセンスと同じ構成を持つ。

【0138】バイディング鍵Kbは、ソフトウェアによって取得された暗号化コンテンツデータのライセンスを管理するものであり、ハードウェアによって保持される。そして、ハードウェアによって保持されたバイディング鍵Kbによらなければライセンスを取出すことができないものである。また、制御情報ACmb、ACpbは、暗号化コンテンツデータを再生するライセンスに含まれるACm、ACPに相当するもので、固定値を持つ。ACmbは、ライセンスの再生回数制限無し、移動複製禁止、かつ、セキュリティレベル1を表し、ACpbは、再生期限が無期限であることを表す。

【0139】チェックアウト管理情報は、チェックアウト可能数と、チェックアウト先個別IDと、チェックアウト時トランザクションIDとから成る。チェックアウト可能数は、暗号化コンテンツデータを貸出すことができる回数を示すものであり、暗号化コンテンツデータをチェックアウトする毎に数値が1つ減じられ、暗号化コンテンツデータをチェックインする毎に数値が1つ増加されるものである。また、チェックアウト先個別IDは、暗号化コンテンツデータをチェックアウトするメモリカードを特定する識別情報であり、メモリカードが保持する個別公開暗号鍵Kpmcxが該当する。チェックアウト時トランザクションIDは、チェックアウトするとき用いられるローカル使用のトランザクションIDである。

【0140】図5は、図1に示した配信サーバ10の構成を示す概略ブロック図である。配信サーバ10は、コンテンツデータを所定の方式に従って暗号化したデータや、コンテンツID等の配信情報を保持するための情報データベース304と、パーソナルコンピュータの各ユーザーごとにコンテンツデータへのアクセス開始に従った課金情報を保持するための課金データベース302と、禁止クラスリストCRLを管理するCRLデータベース306と、情報データベース304に保持されたコンテンツデータのメニューを保持するメニューデータベース307と、ライセンスの配信ごとにコンテンツデータおよびライセンス鍵等の配信を特定するトランザクションIDの配信に関する記録して、保持する配信記録データベース308と、情報データベース304、課金データベース302、CRLデータベース306、メニューデ

10

20

30

40

50

ータベース307、および配信記録データベース308からのデータをバスBS1を介して受取り、所定の処理を行なうためのデータ処理部310と、通信網を介して、配信キャリア20とデータ処理部310との間でデータ授受を行なうための通信装置350とを備える。

【0141】データ処理部310は、バスBS1上のデータに応じて、データ処理部310の動作を制御するための配信制御部315と、配信制御部315に制御されて、配信セッション時にセッションキーKs1を発生するためのセッションキー発生部316と、ライセンス管理デバイス、およびライセンス管理モジュールから送られてきた認証のための認証データ{Kpmw/Cmw}Kpaを復号するための公開認証鍵Kpaを保持する認証鍵保持部313と、ライセンス管理デバイス、およびライセンス管理モジュールから送られてきた認証のための認証データ{Kpmw/Cmw}Kpaを通信装置350およびバスBS1を介して受けて、認証鍵保持部313からの公開認証鍵Kpaによって復号処理を行なう復号処理部312と、セッションキー発生部316より生成されたセッションキーKs1を復号処理部312によって得られたクラス公開暗号鍵Kpmwを用いて暗号化して、バスBS1に出力するための暗号化処理部318と、セッションキーKs1によって暗号化された上で送信されたデータをバスBS1より受けて、復号処理を行なう復号処理部320とを含む。

【0142】データ処理部310は、さらに、配信制御部315から与えられるライセンス鍵Kcおよびアクセス制限情報ACmを、復号処理部320によって得られたメモリカード、ライセンス管理デバイス、およびライセンス管理モジュールの個別公開暗号鍵Kpmcxによって暗号化するための暗号化処理部326と、暗号化処理部326の出力を、復号処理部320から与えられるセッションキーKs2によってさらに暗号化してバスBS1に出力するための暗号化処理部328とを含む。

【0143】配信サーバが保持する認証鍵は、配信サーバが配信しようとするライセンスの要求する受信側のセキュリティレベルによって異なる。セキュリティレベル2を要求するレベル2ライセンスを配信する配信サーバにあっては、セキュリティレベルがレベル2の機器が送信してくる認証データに対して認証処理が可能な認証鍵Kpa2を保持する。また、配信しようとするライセンスがセキュリティレベル1を要求するレベル1ライセンスを配信する配信サーバにあっては、セキュリティレベルがレベル2の機器およびセキュリティレベルがレベル1の機器のいずれに対しても配信可能であるため、レベル2およびレベル1のそれぞれに対応した認証鍵Kpa2およびKpa1を保持し、相手のレベルに応じて使い分けることになる。さらには、送信された認証データが必要とする認証鍵は、クラス証明書Cmwの認証データとして暗号化されても、なお、平文として維持される領

域に記載され配信サーバ10の配信制御部315が、復号処理部312にて復号前に容易に認証鍵を特定できる構成となっている。2つの認証鍵を区別するためにレベル2に対応した認証鍵KPa2をレベル2認証鍵KPa2、レベル1に対応した認証鍵KPa1を、レベル1認証鍵KPa1と称し、総じて認証鍵KPaと称する。

【0144】配信サーバ10の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【0145】図6は、図1に示したパーソナルコンピュータ50の構成を説明するための概略ブロック図である。パーソナルコンピュータ50は、パーソナルコンピュータ50の各部のデータ授受を行なうためのバスBS2と、パーソナルコンピュータ内を制御すると共に、各種のプログラムを実行するためのコントローラ(CPU)510と、データバスBS2と、データバスBS2に接続され、プログラムやデータを記録し、蓄積しておくための大容量記録装置であるハードディスク(HDD)530およびCD-ROMドライブ540と、ユーザからの指示を入力するためのキーボード560と、各種の情報を視覚的にユーザに与えるためのディスプレイ570を含む。

【0146】パーソナルコンピュータ50は、さらに、暗号化コンテンツデータおよびライセンスを再生端末100等に通信する際にコントローラ510と端子580との間でデータの授受を制御するためのUSBインタフェース550と、USBケーブル70を接続するための端子580と、配信サーバ10とインターネット網30およびモデム40を介して通信する際にコントローラ510と端子585との間でデータの授受を制御するためのシリアルインタフェース555と、ケーブルによってモデム40と接続するための端子585とを含む。

【0147】コントローラ510は、アプリケーションプログラムを実行することで、インターネット網30を介してライセンス管理デバイス520またはライセンス管理モジュール511に暗号化コンテンツデータ等を配信サーバ10から受信するために、配信サーバ10との間でデータの授受を制御するとともに、CD-ROMドライブ540を介して音楽CDからリッピングによって暗号化コンテンツデータおよびライセンスを取得する際の制御を行なう。

【0148】さらに、パーソナルコンピュータ50は、配信サーバ10からの暗号化コンテンツデータおよびライセンスの受信を行なう際に配信サーバ10との間で各種の鍵のやり取りを行ない、配信された暗号化コンテンツデータを再生するためのライセンスをハード的に管理するライセンス管理デバイス520と、コントローラ510にて実行されるプログラムであって、配信サーバ10からの暗号化コンテンツデータおよびレベル1ライセンスの受信をプログラムによって実行し、受信したライ

センスに独自の暗号化を施した専用ライセンスを生成するコンテンツ管理モジュール511とを含む。

【0149】ライセンス管理デバイス520は、暗号化コンテンツデータおよびライセンスを配信サーバ10から受信する際のデータの授受をハード的に行ない、受信したライセンスをハード的に管理するものであるため、高いセキュリティレベルを要求するレベル2のライセンスを扱うことが出来る。一方、ライセンス管理モジュール511は、暗号化コンテンツデータおよびライセンスを配信サーバ10から受信する際のデータの授受をコンロとローラ510にて実行されるプログラムを用いてソフト的に行ない、ライセンスの受信を、また、音楽CDからリッピングによってローカル使用の暗号化コンテンツデータおよびライセンスの生成を行い、取得したライセンスに対して暗号処理などを施して保護し、HDD530に蓄積して管理するものであるため、ライセンス管理デバイス520よりもセキュリティレベルが低い、レベル1ライセンスのみを扱う。なお、高いセキュリティレベルがレベル2である場合にはレベル1ライセンスも扱えることは言うまでもない。

【0150】このように、パーソナルコンピュータ50は、配信サーバ10からインターネット網30を介して暗号化コンテンツデータおよびライセンスを受信するためのライセンス管理モジュール511およびライセンス管理デバイス520と、音楽CDからリッピングによって暗号化コンテンツデータおよびライセンスを取得するためのCD-ROMドライブ540とを内蔵するものである。

【0151】図7は、図1に示した再生端末100の構成を説明するための概略ブロック図である。

【0152】再生端末100は、再生端末100の各部のデータ授受を行なうためのバスBS3と、バスBS3を介して再生端末100の動作を制御するためのコントローラ1106と、外部からの指示を再生端末100に与えるための操作パネル1108と、コントローラ1106等から出力される情報を携帯電話ユーザに視覚情報として与えるための表示パネル1110とを含む。

【0153】再生端末100は、さらに、配信サーバ10からのコンテンツデータ(音楽データ)を記憶しかつ復号化処理するための着脱可能なメモ리카ード110と、メモ리카ード110とバスBS3との間のデータの授受を制御するためのメモリインタフェース1200と、パーソナルコンピュータ50から暗号化コンテンツデータおよびライセンスを受信する際にバスBS3と端子1114との間のデータ授受を制御するためのUSBインタフェース1112と、USBケーブル70を接続するための端子1114とを含む。

【0154】再生端末100は、さらに、再生端末の種類(クラス)ごとにそれぞれ設定される、クラス公開暗号鍵Kp1およびクラス証明書Cp1をクラス公開認



証鍵KPaで復号することでその正当性を認証できる状態に暗号化した認証データ{Kppl/Cpl}KPa2を保持する認証データ保持部1500を含む。ここで、再生端末100のクラスyは、y=1であるとする。また、再生端末は、ハード的に機密性を保持できるコンテンツ再生デバイスを用いて再生を提供する機器であるためセキュリティレベルはレベル2である。

【0155】再生端末100は、さらに、再生端末(コンテンツ再生デバイス)のクラス秘密復号鍵であるKp1を保持するKp1保持部1502と、バスBS3から受けたデータをKp1によって復号しメモリカード110によって発生されたセッションキーKs2を得る復号処理部1504とを含む。

【0156】再生端末100は、さらに、メモリカード110に記憶されたコンテンツデータの再生を行なう再生セッションにおいてメモリカード110との間でバスBS3上においてやり取りされるデータを暗号化するためのセッションキーKs3を乱数等により発生するセッションキー発生部1508と、暗号化コンテンツデータの再生セッションにおいてメモリカード110からライセンス鍵Kcおよび再生期限ACpを受取る際に、セッションキー発生部1508により発生されたセッションキーKs3を復号処理部1504によって得られたセッションキーKs2によって暗号化しバスBS3に出力する暗号化処理部1506とを含む。

【0157】再生端末100は、さらに、バスBS3上のデータをセッションキーKs3によって復号して、ライセンス鍵Kcおよび再生期限ACpを出力する復号処理部1510と、バスBS3より暗号化コンテンツデータ(Dc)Kcを受けて、復号処理部1510より取得したライセンス鍵Kcによって復号しコンテンツデータを出力する復号処理部1516と、復号処理部1516の出力を受けてコンテンツデータを再生するための音楽再生部1518と、音楽再生部1518の出力をデジタル信号からアナログ信号に変換するDA変換器1519と、DA変換器1519の出力をヘッドホンなどの外部出力装置(図示省略)へ出力するための端子1530とを含む。

【0158】なお、図7においては、点線で囲んだ領域は暗号化コンテンツデータを復号して音楽データを再生するコンテンツ再生デバイス1550を構成する。また、図7においては、説明の簡素化のため、再生端末のうち本発明の音楽データの再生にかかわるブロックのみを記載し、再生端末が本来備えている通話機能に関するブロックについては、一部記載を省略している。

【0159】再生端末100の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【0160】図8は、メモリカード110の構成を説明するための概略ブロック図である。既に説明したよう

に、メモリカードに固有の公開暗号鍵および秘密復号鍵として、KpmwおよびKmwが設けられ、メモリカードのクラス証明書Cmwが設けられるが、メモリカード110においては、メモリカードのクラスを識別する自然数w=3で、メモリカードを識別する自然数x=4でそれぞれ表わされるものとする。また、メモリカード110は、ハード的に機密性を保持する機器であるためセキュリティレベルは2である。

【0161】したがって、メモリカード110は、認証データ{Kpm3/Cm3}KPa2を保持する認証データ保持部1400と、メモリカードごとに設定される固有の復号鍵である個別秘密復号鍵Kmc4を保持するKmc保持部1402と、メモリカードの種類ごとに設定される固有のクラス秘密復号鍵Km3を保持するKm保持部1421と、個別秘密復号鍵Kmc4によって復号可能な公開暗号鍵Kpmc4を保持するKpmc保持部1416とを含む。

【0162】このように、メモリカードという記録装置の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたライセンス鍵の管理をメモリカード単位で実行することが可能になる。

【0163】メモリカード110は、さらに、メモリインタフェース1200との間で信号を端子1426を介して授受するインタフェース1424と、インタフェース1424との間で信号をやり取りするバスBS4と、バスBS4にインタフェース1424から与えられるデータから、メモリカードの種類ごとに固有のクラス秘密復号鍵Km3をKm保持部1421から受けて、配信サーバ10が配信セッションにおいて生成したセッションキーKs1を接点Paに出力する復号処理部1422と、KPa保持部1414からレベル2認証鍵KPa2を受けて、バスBS4に与えられるデータからレベル2認証鍵KPa2による復号処理を実行して復号結果と得られたクラス証明書をコントローラ1420に、得られたクラス公開鍵を暗号化処理部1410に出力する復号処理部1408と、切換スイッチ1442によって選択的に与えられる鍵によって、切換スイッチ1446によって選択的に与えられるデータを暗号化してバスBS4に出力する暗号化処理部1406とを含む。

【0164】メモリカード110は、さらに、各セッションにおいてセッションキーKs2を発生するセッションキー発生部1418と、セッションキー発生部1418の出力したセッションキーKs2を復号処理部1408によって得られるクラス公開暗号鍵KppyもしくはKpmwによって暗号化してバスBS4に送出する暗号化処理部1410と、バスBS4よりセッションキーKs2によって暗号化されたデータを受けてセッションキー発生部1418より得たセッションキーKs2によって復号する復号処理部1412と、暗号化コンテンツデ

ータの再生セッションにおいてメモリ1415から読出されたライセンス鍵Kcおよび再生期限ACpを、復号処理部1412で復号された他のメモリカード110に固有の個別公開暗号鍵Kpmcx(≠4)で暗号化する暗号処理部1417とを含む。

【0165】メモリカード110は、さらに、バスBS4上のデータを個別公開暗号鍵Kpmc4と対をなすメモリカード110固有の個別秘密復号鍵Kmc4によって復号するための復号処理部1404と、禁止クラスリストデータCRLと、暗号化コンテンツデータ{Dc}Kcと、暗号化コンテンツデータ{Dc}Kcを再生するためのライセンス(Kc, ACp, ACm, ライセンスID)と、付加情報Data-infと、暗号化コンテンツデータの再生リストファイルと、ライセンスを管理するためのライセンス管理ファイルとをバスBS4より受けて格納するためのメモリ1415とを含む。メモリ1415は、例えば半導体メモリによって構成される。また、メモリ1515は、禁止クラスリストCRLを記録するためのCRL領域1415Aと、ライセンスを記録するライセンス領域1415Bと、暗号化コンテンツデータ{Dc}Kc、暗号化コンテンツデータの関連情報Dc-inf、メモリカードに記録された暗号化コンテンツデータやライセンスをアクセスするための基本的な情報を記録する再生リストファイル、およびライセンスを管理するために必要な情報を暗号化コンテンツデータごとに記録するライセンス管理ファイルを記録する外部から直接アクセスが可能なデータ領域1415Cとから成る。ライセンス管理ファイルおよび再生リストファイルの詳細については後述する。

【0166】また、ライセンス領域1415Bは、ライセンス(コンテンツ鍵Kc、再生制御情報ACp、アクセス制限情報ACm、ライセンスID)を記録するためにエントリと呼ばれるライセンス専用の記録単位でライセンスを格納する。ライセンスに対してアクセスする場合には、ライセンスが格納されている、あるいは、ライセンスを記録したいエントリをエントリ番号によって指定する構成になっている。

【0167】メモリカード110は、さらに、バスBS4を介して外部との間でデータ授受を行ない、バスBS4との間で再生情報等を受けて、メモリカード110の動作を制御するためのコントローラ1420とを含む。

【0168】なお、データ領域1415Cを除く全ての構成は、耐タンボモジュール領域に構成される。

【0169】図9は、パーソナルコンピュータ50に内蔵されたライセンス管理デバイス520の構成を示す概略ブロック図である。ライセンス管理デバイス520は、メモリカード110におけるデータ領域1415Cに相当する領域を必要としない点、インタフェース1424の機能および端子1426の形状が異なるインタフェース5224と端子5226とを備える点が異なるのみ

で、基本的にメモリカード110と同じ構成から成る。ライセンス管理デバイス520の認証データ保持部5200、Kmc保持部5202、復号処理部5204、暗号処理部5206、復号処理部5208、暗号処理部5210、復号処理部5212、KPa保持部5214、Kpmc保持部5216、暗号処理部5217、セッションキー発生部5218、コントローラ5220、Km保持部5221、復号処理部5222、インタフェース5224、端子5226、切換スイッチ5242、5246は、それぞれ、メモリカード110の認証データ保持部1400、Kmc保持部1402、復号処理部1404、暗号処理部1406、復号処理部1408、暗号処理部1410、復号処理部1412、KPa保持部1414、Kpmc保持部1416、暗号処理部1417、セッションキー発生部1418、コントローラ1420、Km保持部1421、復号処理部1422、切換スイッチ1442、1446と同じである。ただし、認証データ保持部5200は、認証データ{Kpm7/Cm7}KPa2を保持し、Kpmc保持部5216は、個別公開暗号鍵Kpm8を保持し、Km保持部5202は、クラス秘密復号鍵Km7を保持し、Kmc保持部5221は、個別秘密復号鍵Kmc8を保持する。ライセンス管理デバイス520のクラスを表す自然数wはw=7であり、ライセンス管理デバイス520を識別するための自然数xはx=8であるとする。

【0170】ライセンス管理デバイス520は、禁止クラスリストCRLとライセンス(Kc, ACp, ACm, ライセンスID)とを記録するメモリ5215を、メモリカード110のメモリ1415に代えて含む。メモリ5215は、禁止クラスリストCRLを記録したCRL領域5215Aと、ライセンスを記録したライセンス領域5215Bとから成る。

【0171】さらに、ライセンス管理デバイス520は、ライセンス管理モジュール511が利用するバインディングライセンスを保持する必要がある。したがって、KPa保持部5214は、2つの認証鍵KPa2およびKPa1を保持する。異なるレベルからの制御については、後ほどフローチャートを使用して詳細に説明する。

【0172】更に、ライセンス管理モジュール511はライセンスを管理するプログラムであり、セキュリティレベルは1である。また、ライセンス管理モジュール511は、ライセンス管理デバイス520とほぼ同一の構成を持つ管理プログラムなのでライセンス管理モジュール511のクラスを表す自然数wはw=5であり、ライセンス管理デバイス520を識別するための自然数xはx=6であるとする。したがって、ライセンス管理モジュール511は、認証データ{Kpm5/Cm5}KPa1、個別公開暗号鍵Kpm6、クラス秘密復号鍵Km5、個別秘密復号鍵Kmc6を保持する。また、2つ

の認証鍵KPa2およびKPa1を保持する。

【0173】以下、図1に示すデータ配信システムにおける各セッションの動作について説明する。

【0174】〔初期化〕パーソナルコンピュータ50が配信サーバ10から暗号化コンテンツデータおよびライセンスの配信を受ける前に行なわれる初期化について説明する。

【0175】図10～図12は、パーソナルコンピュータ50が暗号化コンテンツデータおよびライセンスを配信サーバ10から受信する前に行なわれる初期化を説明するための第1～第3のフローチャートである。

【0176】図10を参照して、バイディングライセンスの生成がキーボード560を介してリクエストされると(ステップS10)、ライセンス管理モジュール511は、バイディング鍵Kbを生成し(ステップS12)、次いで、トランザクションIDb、コンテンツIDb、所定の制御情報ACmbおよびACpbを生成する(ステップS14)。ステップS12、S14はバイディングライセンスの生成処理である。

【0177】そして、ライセンス管理モジュール511は、ライセンス管理デバイス520に対してバスBS2を介して認証データの出力を指示する(ステップS16)。

【0178】そうすると、ライセンス管理デバイス520のコントローラ5220は、端子5226、インタフェース5224、およびバスBS5を介して認証データの出力指示を受取り、認証データ保持部5200からバスBS5を介して認証データ{Kpm7//Cm7}KPa2を取得し、バスBS5、インタフェース5224および端子5226を介して認証データ{Kpm7//Cm7}KPa2を出力する(ステップS18)。ライセンス管理モジュール511は、バスBS2を介して認証データ{Kpm7//Cm7}KPa2を受信し(ステップS20)、認証データ{Kpm7//Cm7}KPaをレベル2認証鍵KPa2によって復号する(ステップS22)。

【0179】ライセンス管理モジュール511は、復号処理結果から、処理が正常に行なわれたか否か、すなわち、ライセンス管理デバイス520が正規のライセンス管理デバイスからの公開暗号鍵Kpm7と証明書Cm7とを保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう(ステップS24)。正当な認証データであると判断された場合、ライセンス管理モジュール511は、公開暗号鍵Kpm7および証明書Cm7を承認し、受理する。そして、次の処理(ステップS26)へ移行する。正当な認証データでない場合には、非承認とし、公開暗号鍵Kpm7および証明書Cm7を受理しないで処理を終了する(ステップS68)。

【0180】認証の結果、正規の機器であることが認識されると、ライセンス管理モジュール511は、次に、ライセンス管理デバイスのクラス証明書Cm7が禁止クラスリストCRLにリストアップされているかどうかをハードディスク(HDD)530に照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここで初期化を終了する(ステップS68)。

【0181】一方、ライセンス管理デバイス520のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する(ステップS26)。

【0182】認証の結果、正当な認証データを持つライセンス管理デバイスからのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、ライセンス管理モジュール511は、セッションキーKs2aを生成する(ステップS28)。

【0183】図11を参照して、ライセンス管理モジュール511は、セッションキーKs2aをクラス公開暗号鍵Kpm7によって暗号化して暗号化データ{Ks2a}Km7を生成し(ステップS30)、暗号化データ{Ks2a}Km7をバスBS2を介してライセンス管理デバイス520へ出力する(ステップS32)。ライセンス管理デバイス520のコントローラ5220は、端子5226、インタフェース5224、およびバスBS5を介して暗号化データ{Ks2a}Km7を受け、復号処理部5222は、Km保持部5221から出力されるクラス秘密復号鍵Km7によって暗号化データ{Ks2a}Km7を復号してセッションキーKs2aを受理する(ステップS34)。コントローラ5220は、セッションキーKs2aを受理したことに伴い、セッションキー発生部5218を制御してセッションキーKs2bを発生させる。そうすると、セッションキー発生部5218は、セッションキーKs2bを生成し(ステップS36)、コントローラ5220は、バスBS5を介してメモリ5215のCRL領域5215Aから禁止クラスリストCRLの更新日時CRLdateを取得し、その取得した更新日時CRLdateをバスBS5を介して切換スイッチ5246へ出力する(ステップS38)。そうすると、暗号処理部5206は、切換スイッチ5246を順次切換えることによって受取ったセッションキーKs2b、個別公開暗号鍵Kpmc8および更新日時CRLdateを復号処理部5222からのセッションキーKs2aによって暗号化する。コントローラ5220は、バスBS5上の暗号化データ{Ks2b//Kpmc8//CRLdate}Ks2aをインタフェース5224および端子5226を介して出力する(ステップS40)。

【0184】ライセンス管理モジュール511は、バスBS2を介して暗号化データ{Ks2b//Kpmc8//CRLdate}Ks2aを受取り、暗号化データ{Ks2b//Kpmc8//CRLdate}Ks2

aをセッションキーKs2aによって復号してセッションキーKs2b、個別公開暗号鍵Kpmc8、および更新日時CRLdateを受理する(ステップS42)。そして、ライセンス管理モジュール511は、ステップS12、S14で生成したバイディングライセンス(トランザクションIDb、コンテンツIDb、バイディング鍵Kb、および制御情報ACmb、ACpb)を公開暗号鍵Kpmc8によって暗号化して暗号化データ{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8を生成する(ステップS44)。

【0185】図12を参照して、ライセンス管理モジュール511において、ライセンス管理デバイス520から送信された禁止クラスリストの更新日時CRLdateがハードディスク(HDD)530に保持されている禁止クラスリストCRLの更新日時から、いずれが保持する禁止クラスリストが新しいかが比較される。ライセンス管理デバイス520の禁止クラスリストCRLの方が新しいとき、ステップS48へ移行する。また、逆に、ライセンス管理モジュール511の禁止クラスリストCRLの方が新しいときはステップS52へ移行する(ステップS46)。

【0186】ライセンス管理デバイス520の禁止クラスリストCRLの方が新しいと判断されたとき、ライセンス管理モジュール511は、暗号化データ{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8をライセンス管理デバイス520において発生されたセッションキーKs2bによって暗号化を行い、暗号化データ{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8}Ks2bをバスBS2を介してライセンス管理デバイス520へ出力する(ステップS48)。

【0187】そして、ライセンス管理デバイス520のコントローラ5220は、暗号化データ{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8}Ks2bを端子5226およびインタフェース5224を介して受取り、セッションキー発生部5218によって発生されたセッションキーKs2bによって復号し、{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8を受理する(ステップS50)。その後、ステップS60へ移行する。

【0188】一方、ライセンス管理モジュール511において、ライセンス管理モジュール511の禁止クラスリストCRLの方が新しいと判断されると、ライセンス管理モジュール511は、ライセンス管理デバイス520が保持する禁止クラスリストCRLを更新するため、バスBS2を介してHDD530から更新日時CRLdate以降の更新分を差分CRLとして取得する(ステ

ップS52)。

【0189】そして、ライセンス管理モジュール511は、禁止クラスリストの差分CRLと暗号化データ{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8とを、ライセンス管理デバイス520において生成されたセッションキーKs2bによって暗号化し、暗号化データ{CRLdate//{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8}Ks2bをバスBS2を介してライセンス管理デバイス520へ出力する(ステップS54)。

【0190】ライセンス管理デバイス520のコントローラ5220は、端子5226およびインタフェース5224を介して、バスBS5に与えられた受信データを復号処理部5212によって復号する。復号処理部5212は、セッションキー発生部5218から与えられたセッションキーKs2bを用いてバスBS5の受信データを復号しバスBS5に出力する(ステップS56)。

【0191】この段階で、バスBS5には、Kmc保持部5221に保持される個別秘密復号鍵Kmc8で復号可能な{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8と、差分CRLとが出力される(ステップS56)。コントローラ5220の指示によって受理した差分CRLによってメモリ5215内のCRL領域5215Aを差分CRLに基づいて更新する(ステップS58)。

【0192】ステップS48、S50は、送信側のライセンス管理モジュール511の禁止クラスリストCRLより、受信側のライセンス管理デバイス520の禁止クラスリストCRLが新しい場合のバイディング鍵Kb等のライセンス管理デバイス520への送信動作であり、ステップS52、S54、S56、S58は、受信側のライセンス管理デバイス520の禁止クラスリストCRLより、送信側のライセンス管理モジュール511の禁止クラスリストCRLが新しい場合のバイディング鍵Kb等のライセンス管理デバイス520への送信動作である。このように、ライセンス管理デバイス520から送られてきた禁止クラスリストの更新日時CRLdateを比較し、受信側の禁止クラスリストCRLが送信側の禁止クラスリストCRLより古いとき、禁止クラスリストの差分データである差分CRLをHDD530から取得し、差分CRLをライセンス管理デバイス520に配信することによって、常に新しい禁止クラスリストCRLを保持させるようにしている。

【0193】ステップS50またはステップS58の後、コントローラ5220の指示によって、暗号化データ{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8は、復号処理部5204において、秘密復号鍵Kmc8によって復号され、バイディングライセンス(バイディング鍵K

10

20

30

40

50

b、トランザクションIDb、コンテンツIDb、制御情報ACmZ、ACp)が受理される(ステップS60)。

【0194】そして、ライセンス管理モジュール511は、バイディングライセンスを格納するためのエン트리番号「0」をライセンス管理デバイス520へ入力し(ステップS62)、ライセンス管理デバイス520のコントローラ5220は、端子5226、インタフェース5224、およびバスBS5を介してエン트리番号「0」を受取り、メモリ5215のライセンス領域5215Bのうち、受取ったエン트리番号「0」によって指定された領域にバイディングライセンス(トランザクションIDb、コンテンツIDb、バイディング鍵Kb、制御情報ACmb、ACpb)を格納する(ステップS64)。

【0195】ライセンス管理モジュール511が、バイディング鍵Kbを記録するためにライセンス管理デバイス520の領域を確認し、登録の準備を行なう図10のステップ16から図11のステップ42までの一連の処理を「デバイス確認処理」、バイディング鍵Kbをライセンス管理デバイス520のライセンス領域5215Bに格納する図11のステップS44から図12のステップS64までの一連の処理を「バイディング鍵登録処理」と称する。

【0196】一方、ライセンス管理モジュール511は、機密情報(レベル1ライセンスおよびチェックアウト情報)が空な平文の機密ファイルを生成し、バイディング鍵Kbによって機密ファイルを暗号化した暗号化機密ファイル160を生成して暗号化機密ファイル160をHDD530に記録し(ステップS66)、初期化の動作を終了する(ステップS68)。

【0197】このように、パーソナルコンピュータ50のライセンス管理モジュール511は、初期化動作において、バイディングライセンスを生成し、ライセンス管理デバイス520におけるメモリ5215のライセンス領域5215Bのうち、エン트리番号「0」によって指定される領域に生成したバイディングライセンスを格納するとともに、生成したバイディングライセンスに含まれるバイディング鍵Kbによって機密ファイルを暗号化した暗号化機密ファイル160を生成する。そして、この暗号化機密ファイル160は、ライセンス管理モジュール511によって配信サーバ10から受信したライセンスを格納するためのものである。また、このようにバイディング鍵Kbによって機密ファイルを暗号化することによりバイディング鍵Kbがないと暗号化機密ファイル160からライセンスを取出すことができないため、バイディング鍵Kbは暗号化コンテンツデータのライセンスを管理するための共通鍵である。そして、このバイディング鍵Kbはライセンス管理デバイス520のメモリ5215に格納されているため、バ

ィング鍵Kbをハードウェアによって管理することができる。その結果、バイディング鍵Kbを介してHDD530に記録された暗号化機密ファイル160でソフト的に管理される暗号化コンテンツデータのライセンスをハードウェアによって管理することになる。したがって、後述するように、ソフトウェアによって受信された暗号化コンテンツデータおよびライセンスを他のパーソナルコンピュータ80へ移動できる。

【0198】[配信1]次に、図1に示すデータ配信システムにおいて、配信サーバ10からパーソナルコンピュータ50のライセンス管理デバイス520へ暗号化コンテンツデータおよびセキュリティレベル2を要求するレベル2ライセンスを配信する動作について説明する。なお、この動作を「配信1」という。

【0199】図13～図16は、図1に示すデータ配信システムにおける暗号化コンテンツデータの購入時に発生するパーソナルコンピュータ50に内蔵されたライセンス管理デバイス520への配信動作(以下、配信セッションともいう)を説明するための第1～第4のフローチャートである。

【0200】図13における処理以前に、パーソナルコンピュータ50のユーザは、配信サーバ10に対してモデム40を介して接続し、購入を希望するコンテンツに対するコンテンツIDを取得していることを前提としている。

【0201】図13を参照して、パーソナルコンピュータ50のユーザからキーボード560を介してコンテンツIDの指定による配信リクエストがなされる(ステップS100)。そして、キーボード560を介して暗号化コンテンツデータのライセンスを購入するための購入条件ACが入力される(ステップS102)。つまり、選択した暗号化コンテンツデータを復号するライセンス鍵Kcを購入するために、暗号化コンテンツデータのアクセス制限情報ACm、および再生期限ACpを設定して購入条件ACが入力される。

【0202】暗号化コンテンツデータの購入条件ACが入力されると、コントローラ510は、バスBS2を介してライセンス管理デバイス520へ認証データの出力指示を与える(ステップS104)。ライセンス管理デバイス520のコントローラ5220は、端子5226、インタフェース5224およびバスBS5を介して認証データの出力指示を受取る。そして、コントローラ5220は、バスBS5を介して認証データ保持部5200から認証データ{Kpm7//Cm7}KPa2を読み出し、{Kpm7//Cm7}KPa2をバスBS5、インタフェース5224および端子5226を介して出力する(ステップS106)。

【0203】パーソナルコンピュータ50のコントローラ510は、ライセンス管理デバイス520からの認証データ{Kpm7//Cm7}KPa2に加えて、コン

テンツID、ライセンス購入条件のデータAC、および配信リクエストを配信サーバ10に対して送信する(ステップS108)。

【0204】配信サーバ10では、パーソナルコンピュータ50から配信リクエスト、コンテンツID、認証データ{KPa2/／Cm7}KPa2、およびライセンス購入条件のデータACを受信し(ステップS110)、復号処理部312においてライセンス管理デバイス520から出力された認証データをレベル2認証鍵KPaで復号処理を実行する(ステップS112)。

【0205】配信制御部315は、復号処理部312における復号処理結果から、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう(ステップS114)。正当な認証データであると判断された場合、配信制御部315は、クラス公開暗号鍵KPa7およびクラス証明書Cm7を承認し、受理する。そして、次の処理(ステップS116)へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵KPa7およびクラス証明書Cm7を受理しないで配信セッションを終了する(ステップS198)。仮に、レベル1からの配信要求を行っていたとすると、レベル2認証鍵KPa2では、レベル1の認証データを認証することができないためここで処理は終了する。

【0206】認証の結果、正規の認証データであり、クラス公開暗号鍵KPa7およびクラス証明書Cm7を承認されると、配信制御部315は、次に、ライセンス管理デバイスのクラス証明書Cm7が禁止クラスリストCRLにリストアップされているかどうかをCRLデータベース306に照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここで配信セッションを終了する(ステップS198)。

【0207】一方、ライセンス管理デバイス520のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する(ステップS116)。

【0208】認証の結果、正当な認証データを持つライセンス管理デバイスを備えるパーソナルコンピュータからのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、配信サーバ10において、配信制御部315は、配信を特定するための管理コードであるトランザクションIDを生成する(ステップS118)。また、セッションキー発生部316は、配信のためのセッションキーKs1を生成する(ステップS120)。セッションキーKs1は、復号処理部312によって得られたライセンス管理デバイス520に対応するクラス公開暗号鍵KPa7によって、暗号化処理部318によって暗号化される(ステップS122)。

【0209】トランザクションIDおよび暗号化されたセッションキーKs1は、トランザクションID／／{Ks1}Km7として、バスBS1および通信装置3

50を介して外部に出力される(ステップS124)。

【0210】図14を参照して、パーソナルコンピュータ50が、トランザクションID／／{Ks1}Km7を受信すると(ステップS126)、コントローラ510は、トランザクションID／／{Ks1}Km7をライセンス管理デバイス520に入力する(ステップS128)。そうすると、ライセンス管理デバイス520においては、端子5226およびインタフェース5224を介して、バスBS5に与えられた受信データを、復号処理部5222が、保持部5221に保持されるライセンス管理デバイス520にクラス秘密復号鍵Km7により復号処理することにより、セッションキーKs1を復号し、セッションキーKs1を受理する(ステップS130)。

【0211】コントローラ5220は、配信サーバ10で生成されたセッションキーKs1の受理を確認すると、セッションキー発生部5218に対してライセンス管理デバイス520において配信動作時に生成されるセッションキーKs2の生成を指示する。そして、セッションキー発生部5218は、セッションキーKs2を生成する(ステップS132)。

【0212】また、配信セッションにおいては、コントローラ5220は、ライセンス管理デバイス520内のメモリ5215に記録されている禁止クラスリストCRLから更新日時CRLdateをメモリ1415から抽出して切換スイッチ5246に出力する(ステップS134)。

【0213】暗号化処理部5206は、切換スイッチ5242の接点Paを介して復号処理部5222より与えられるセッションキーKs1によって、切換スイッチ5246の接点を順次切換えることによって与えられるセッションキーKs2、個別公開暗号鍵KPa8および禁止クラスリストの更新日時CRLdateを1つのデータ列として暗号化して、{Ks2／／KPa8／／CRLdate}Ks1をバスBS3に出力する(ステップS136)。

【0214】バスBS3に出力された暗号化データ{Ks2／／KPa8／／CRLdate}Ks1は、バスBS3からインタフェース5224および端子5226を介してパーソナルコンピュータ50に出力され、パーソナルコンピュータ50から配信サーバ10に送信される(ステップS138)。

【0215】配信サーバ10は、トランザクションID／／{Ks2／／KPa8／／CRLdate}Ks1を受信して、復号処理部320においてセッションキーKs1による復号処理を実行し、ライセンス管理デバイス520で生成されたセッションキーKs2、ライセンス管理デバイス520固有の個別公開暗号鍵KPa8およびライセンス管理デバイス520における禁止クラスリストの更新日時CRLdateを受理する(ステ

10

20

30

40

50

ップS142)。

【0216】配信制御部315は、ステップS110で取得したコンテンツIDおよびライセンス購入条件ACに従って、アクセス制限情報ACmおよび再生期限ACpを生成する(ステップS144)。さらに、暗号化コンテンツデータを復号するためのライセンス鍵Kcを情報データベース304より取得する(ステップS146)。

【0217】配信制御部315は、生成したライセンス、すなわち、トランザクションID、コンテンツID、ライセンス鍵Kc、再生期限ACp、およびアクセス制限情報ACmを暗号化処理部326に与える。暗号化処理部326は、復号処理部320によって得られたライセンス管理デバイス520固有の個別公開暗号鍵Kpmc8によってライセンスを暗号化して暗号化データ{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8を生成する(ステップS148)。

【0218】図15を参照して、配信サーバ10において、ライセンス管理デバイス520から送信された禁止クラスリストの更新日時CRLdateを、CRLデータベース306に保持される配信サーバ10の禁止クラスリストCRLの更新日時と比較することによって、ライセンス管理デバイス520は保持する禁止クラスリストCRLが最新か否かが判断され、最新と判断されたとき、ステップS152へ移行する。また、最新でないときはステップS160へ移行する(ステップS150)。

【0219】最新と判断されたとき、暗号化処理部328は、暗号化処理部326から出力された暗号化データ{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8をライセンス管理デバイス520において発生されたセッションキーKs2によって暗号化を行い、暗号化データ{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2をバスBS1に出力する。そして、配信制御部315は、バスBS1上の暗号化データ{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2を通信装置350を介してパーソナルコンピュータ50へ送信する(ステップS152)。

【0220】そして、パーソナルコンピュータ50のコントローラ510は、暗号化データ{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2を受信し(ステップS154)、バスBS5を介してライセンス管理デバイス520に入力する。ライセンス管理デバイス520の復号処理部5212は、暗号化データ{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2を端子5226およびインタフェース522

4を介して受取り、セッションキー発生部5218によって発生されたセッションキーKs2によって復号し、{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8を受理する(ステップS158)。その後、ステップS172へ移行する。

【0221】一方、最新でないと判断されると、配信制御部315は、バスBS1を介してCRLデータベース306から最新の禁止クラスリストCRLを取得し、差分データである差分CRLを生成する(ステップS160)。

【0222】暗号化処理部328は、暗号化処理部326の出力と、配信制御部315がバスBS1を介して供給する禁止クラスリストの差分CRLとを受けて、ライセンス管理デバイス520において生成されたセッションキーKs2によって暗号化する。暗号化処理部328より出力された暗号化データ{差分CRL//{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2は、バスBS1および通信装置350を介してパーソナルコンピュータ50に送信される(ステップS162)。

【0223】パーソナルコンピュータ50は、送信された暗号化データ{差分CRL//{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2を受信し(ステップS164)、バスBS5を介してライセンス管理デバイス520に入力する(ステップS166)。ライセンス管理デバイス520においては、端子5226およびインタフェース5224を介して、バスBS5に与えられた受信データを復号処理部5212によって復号する。復号処理部5212は、セッションキー発生部5218から与えられたセッションキーKs2を用いてバスBS5の受信データを復号しバスBS5に出力する(ステップS168)。

【0224】この段階で、バスBS5には、Kmc保持部5221に保持される秘密復号鍵Kmc8で復号可能な暗号化ライセンス{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8と、差分CRLとが出力される(ステップS168)。コントローラ5220の指示によって受理した差分CRLによってメモリ5215内のCRL領域5215Aを差分CRLに基づいて更新する(ステップS170)。

【0225】ステップS152、S154、S156、S158は、ライセンス管理デバイス520が保持する禁止クラスリストCRLが最新の場合のライセンス鍵Kc等のライセンス管理デバイス520への配信動作であり、ステップS160、S162、S164、S166、S168、S170は、ライセンス管理デバイス520が保持する禁止クラスリストCRLが最新でない場合のライセンス鍵Kc等のライセンス管理デバイス520への配信動作である。このように、ライセンス管理デバイス520から送られてきた禁止クラスリストの更新

日時CRLdateが最新の更新日時か否かを、逐一、確認し、最新でないとき、最新の禁止クラスリストCRLdateをCRLデータベース306から取得し、差分CRLをライセンス管理デバイス520に配信することによって、ライセンスの破られたライセンス管理デバイスへの配信したライセンスの流出を防止できる。

【0226】ステップS158またはステップS170の後、コントローラ5220の指示によって、暗号化ライセンス{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8は、復号処理部5204において、個別秘密復号鍵Kmc8によって復号され、ライセンス(ライセンス鍵Kc、トランザクションID、コンテンツID、アクセス制限情報ACmおよび再生期限ACp)が受理される(ステップS172)。

【0227】図16を参照して、コントローラ510は、ライセンス管理デバイス520が受理したライセンスを格納するエントリを指示するためのエントリ番号を、ライセンス管理デバイス520に入力する(ステップS174)。そうすると、ライセンス管理デバイス520のコントローラ5220は、端子5226およびインタフェース5224を介してエントリ番号を受取り、その受取ったエントリ番号によって指定されるメモリ5215のライセンス領域5215Bに、ステップS172において取得したライセンス(ライセンス鍵Kc、トランザクションID、コンテンツID、アクセス制限情報ACmおよび再生期限ACp)を格納する(ステップS176)。

【0228】パーソナルコンピュータ50のコントローラ510は、配信サーバ10から送られたトランザクションIDと、暗号化コンテンツデータの配信要求を配信サーバ10へ送信する(ステップS178)。

【0229】配信サーバ10は、トランザクションIDおよび暗号化コンテンツデータの配信要求を受信し(ステップS180)、情報データベース304より、暗号化コンテンツデータ{Dc}Kcおよび付加情報Dc-infを取得して、これらのデータをバスBS1および通信装置350を介して出力する(ステップS182)。

【0230】パーソナルコンピュータ50は、{Dc}Kc//Dc-infを受信して、暗号化コンテンツデータ{Dc}Kcおよび付加情報Dc-infを受信する(ステップS184)。そうすると、コントローラ510は、暗号化コンテンツデータ{Dc}Kcおよび付加情報Dc-infを1つのコンテンツファイルとしてバスBS2を介してハードディスク(HDD)530に記録する(ステップS186)。また、コントローラ510は、ライセンス管理デバイス520に格納されたライセンスのエントリ番号と、平文のトランザクションIDおよびコンテンツIDを含む暗号化コンテンツデータ

{Dc}Kcと付加情報Dc-infに対するライセンス管理ファイルを生成し、バスBS2を介してHDD530に記録する(ステップS188)。さらに、コントローラ510は、HDD530に記録されているコンテンツリストファイルに受理したコンテンツの情報として、記録したコンテンツファイル及びライセンス管理ファイルの名称や、付加情報Dc-infから抽出した暗号化コンテンツデータに関する情報(曲名、アーティスト名)等を追記し(ステップS190)、トランザクションIDと配信受理を配信サーバ10へ送信する(ステップS192)。

【0231】配信サーバ10は、トランザクションID//配信受理を受信すると(ステップS194)、課金データベース302への課金データの格納、およびトランザクションIDの配信記録データベース308への記録が行われて配信終了の処理が実行され(ステップS196)、全体の処理が終了する(ステップS198)。

【0232】このようにして、パーソナルコンピュータ50に内蔵されたライセンス管理デバイス50が正規の認証データを保持する機器であること、同時に、クラス証明書Cm7とともに暗号化して送信できた公開暗号鍵Kpm7が有効であることを確認した上で、クラス証明書Cm7が禁止クラスリスト、すなわち、公開暗号鍵Kpm7による暗号化が破られたクラス証明書リストに記載されていないライセンス管理デバイスからの配信要求に対してのみコンテンツデータを配信することができ、不正なライセンス管理デバイスへの配信および解読されたクラス鍵を用いた配信を禁止することができる。

【0233】また、配信サーバおよびライセンス管理デバイスでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、データ配信システムのセキュリティを向上させることができる。

【0234】また、ライセンス管理デバイス520は、配信サーバ10から暗号化コンテンツデータおよびライセンスを受信する際に、配信サーバ10との間でハード的にデータのやり取りを行ない、暗号化コンテンツデータを再生するためのライセンスをハード的に格納するため、そのセキュリティレベルは高い。したがって、ライセンス管理デバイス520を用いれば、パーソナルコンピュータ50は、セキュリティレベルの高い配信によって暗号化コンテンツデータおよびライセンスを受信するとともに、セキュリティレベルの高いレベル2ライセンスの管理が可能である。

【0235】[配信2]図1に示すデータ配信システムにおいて、配信サーバ10からパーソナルコンピュータ50のライセンス管理モジュール511へ暗号化コンテンツデータおよびライセンスを配信する動作について説



明する。なお、この動作を「配信2」という。

【0236】図17～図21は、図1に示すデータ配信システムにおける暗号化コンテンツデータの購入時に発生するパーソナルコンピュータ50に内蔵されたライセンス管理モジュール511への配信動作を説明するための第1～第5のフローチャートである。なお、ライセンス管理モジュール511は、暗号化コンテンツデータおよびライセンスの配信サーバ10からの受信をプログラムによって実行する。

【0237】図17における処理以前に、パーソナルコンピュータ50のユーザは、配信サーバ10に対してモデム40を介して接続し、購入を希望するコンテンツに対するコンテンツIDを取得していることを前提としている。

【0238】図17を参照して、パーソナルコンピュータ50のユーザからキーボード560を介してコンテンツIDの指定による配信リクエストがなされる(ステップS200)。そして、キーボード560を介して暗号化コンテンツデータのライセンスを購入するための購入条件ACが入力される(ステップS202)。つまり、選択した暗号化コンテンツデータを復号するライセンス鍵Kcを購入するために、暗号化コンテンツデータのアクセス制限情報ACm、および再生期限ACpを設定して購入条件ACが入力される。

【0239】暗号化コンテンツデータの購入条件ACが入力されると、コントローラ510は、ライセンス管理モジュール511から認証データ{Kp m5 / / Cm5} Kpa2を讀出し、その讀出した認証データ{Kp m5 / / Cm5} Kpa2に加えて、コンテンツID、ライセンス購入条件のデータAC、および配信リクエストを配信サーバ10に対して送信する(ステップS204)。

【0240】配信サーバ10では、パーソナルコンピュータ50から配信リクエスト、コンテンツID、認証データ{Kp m5 / / Cm5} Kpa2、およびライセンス購入条件のデータACを受信し(ステップS206)、復号処理部312においてライセンス管理モジュール511から出力された認証データをレベル1認証鍵Kpa1で復号処理を実行する(ステップS208)。

【0241】配信制御部315は、復号処理部312における復号処理結果から、処理が正常に行なわれたか否か、すなわち、正規の機関でクラス公開暗号鍵Kpm5とクラス証明書Cm5の正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう(ステップS210)。正当な認証データであると判断された場合、配信制御部315は、クラス公開暗号鍵Kpm5およびクラス証明書Cm5を承認し、受理する。そして、次の処理(ステップS212)へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵Kpm5およびクラス証明書Cm5を

受理しないで処理を終了する(ステップS288)。

【0242】認証の結果、正規のモジュールであることが認識されると、配信制御部315は、次に、ライセンス管理モジュール511のクラス証明書Cm5が禁止クラスリストCRLにリストアップされているかどうかをCRLデータベース306に照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここで配信セッションを終了する(ステップS288)。

【0243】一方、ライセンス管理モジュール511のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する(ステップS214)。

【0244】認証の結果、正当な認証データを持つライセンス管理モジュールを備えるパーソナルコンピュータからのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、配信サーバ10において、配信制御部315は、配信を特定するための管理コードであるトランザクションIDを生成する(ステップS214)。また、セッションキー発生部316は、配信のためのセッションキーKs1を生成する(ステップS216)。セッションキーKs1は、復号処理部312によって得られたライセンス管理モジュール511に対応するクラス公開暗号鍵Kpm5によって、暗号化処理部318によって暗号化される(ステップS218)。

【0245】トランザクションIDおよび暗号化されたセッションキーKs1は、トランザクションID / / {Ks1} Km5として、バスBS1および通信装置350を介して外部に出力される(ステップS220)。

【0246】図18を参照して、パーソナルコンピュータ50のコントローラ510が、トランザクションID / / {Ks1} Km5を受信すると(ステップS222)、ライセンス管理モジュール511は、{Ks1} Km5を受けて、ライセンス管理モジュール511に固有のクラス秘密復号鍵Km5により復号処理して、セッションキーKs1を受信する(ステップS224)。

【0247】ライセンス管理モジュール511は、配信サーバ10で生成されたセッションキーKs1の受理を確認すると、セッションキーKs2を生成する(ステップS226)。そして、コントローラ510は、バスBS2を介してHDD530に記憶された暗号化CRLを讀出し、ライセンス管理モジュール511は、暗号化CRLを復号して禁止クラスリストCRLを取得し、復号した禁止クラスリストCRLに基づいて禁止クラスリストの更新日時CRLdateを取得する(ステップS228)。ライセンス管理モジュール511は、さらに、配信サーバ10において発生されたセッションキーKs1によって、ライセンス管理モジュール511で発生させたセッションキーKs2、個別公開暗号鍵Kpmc6および禁止クラスリストのデータCRLdateを1つ

のデータ列として暗号化して、{Ks2//KpMc6//CRLdate}Ks1を出力する(ステップS230)。

【0248】コントローラ510は、暗号化データ{Ks2//KpMc6//CRLdate}Ks1にトランザクションIDを加えたトランザクションID//{Ks2//KpMc6//CRLdate}Ks1を配信サーバ10へ送信する(ステップS232)。

【0249】配信サーバ10は、トランザクションID//{Ks2//KpMc6//CRLdate}Ks1を受信して(ステップS234)、復号処理部320においてセッションキーKs1による復号処理を実行し、ライセンス管理モジュール511で生成されたセッションキーKs2、ライセンス管理モジュール511に固有の個別公開暗号鍵KpMc6およびライセンス管理モジュール511における禁止クラスリストの更新日時CRLdateを受信する(ステップS236)。

【0250】配信制御部315は、ステップS206で取得したコンテンツIDおよびライセンス購入条件のデータACに従って、アクセス制限情報ACmおよび再生期間ACpを生成する(ステップS238)。さらに、暗号化コンテンツデータを復号するためのライセンス鍵Kcを情報データベース304より取得する(ステップS240)。

【0251】配信制御部315は、生成したライセンス、すなわち、トランザクションID、コンテンツID、ライセンス鍵Kc、再生期間ACp、およびアクセス制限情報ACmを暗号化処理部326に与える。暗号化処理部326は、復号処理部320によって得られたライセンス管理モジュール511に固有の個別公開暗号鍵KpMc6によってライセンスを暗号化して暗号化データ{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc6を生成する(ステップS242)。

【0252】図19を参照して、配信サーバ10において、ライセンス管理モジュール511から送信された禁止クラスリストの更新日時CRLdateによって、配信を求めてきたライセンス管理デバイス520の禁止クラスリストCRLが最新か否かが判断され、ライセンス管理モジュールの禁止クラスリストCRLが最新と判断されたとき、ステップS246へ移行する。また、最新でないと判断されたときはステップS252へ移行する(ステップS244)。

【0253】最新と判断されたとき、暗号化処理部328は、暗号化処理部326から出力された暗号化データ{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc6をライセンス管理モジュール511において発生されたセッションキーKs2によって暗号化を行い、暗号化データ{{トランザクションID//コンテンツID//Kc//ACm//AC

p}Kmc6}Ks2をバスBS1に出力する。そして、配信制御部315は、バスBS1上の暗号化データ{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc6}Ks2を通信装置350を介してパーソナルコンピュータ50へ送信する(ステップS246)。

【0254】そして、パーソナルコンピュータ50のコントローラ510は、暗号化データ{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc6}Ks2を受信し(ステップS248)、ライセンス管理モジュール511は、暗号化データ{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc6}Ks2をセッションキーKs2によって復号し、{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc6を受信する(ステップS250)。その後、ステップS262へ移行する。

【0255】一方、最新でないと判断されると、配信制御部315は、バスBS1を介してCRLデータベース306から最新の禁止クラスリストCRLを取得し、差分データである差分CRLを生成する(ステップS252)。

【0256】暗号化処理部328は、暗号化処理部326の出力と、配信制御部315がバスBS1を介して供給する禁止クラスリストの差分CRLとを受けて、ライセンス管理モジュール511において生成されたセッションキーKs2によって暗号化する。暗号化処理部328より出力された暗号化データ{差分CRL//{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc6}Ks2は、バスBS1および通信装置350を介してパーソナルコンピュータ50に送信される(ステップS254)。

【0257】パーソナルコンピュータ50は、送信された暗号化データ{差分CRL//{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc6}Ks2を受信し(ステップS256)、ライセンス管理モジュール511は、セッションキーKs2を用いて受信データを復号して差分CRLと暗号化データ{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc6とを受信する(ステップS258)。

【0258】コントローラ510は、HDD530に記録された禁止クラスリストCRLに受信した差分CRLを加え、独自の暗号処理を施し、HDD530内の禁止クラスリストCRLを書換える(ステップS260)。

【0259】ステップS246、S248、S250は、ライセンス管理モジュール511から送られてきた禁止クラスリストの更新日時CRLdateによって、ライセンス管理モジュール511の管理する禁止クラスリストCRLが最新の場合のライセンスのライセンス管

理モジュール511への配信動作であり、ステップS252, S254, S256, S258, S260は、禁止クラスリストCRLが最新でない場合のライセンスのライセンス管理モジュール511への配信動作である。このように、ライセンス管理モジュール511から送られてきた禁止クラスリストの更新日時CRLdateによって、配信を求めてきたライセンス管理デバイス520の禁止クラスリストCRLが最新か否かを、逐一、確認し、最新でないとき、最新の禁止クラスリストCRLをCRLデータベース306から取得し、差分CRLをライセンス管理モジュール511に配信することによって、ライセンス管理モジュールへ配信したライセンスがセキュリティの破られた機器へ流出されるのを防止できる。

【0260】ステップS250またはステップS260の後、暗号化ライセンス{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc6は、個別秘密復号鍵Kmc6によって復号され、ライセンス(ライセンス鍵Kc、トランザクションID、コンテンツID、アクセス制限情報ACmおよび再生期限ACp)が受理される(ステップS262)。

【0261】このように、配信サーバおよびライセンス管理モジュールでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、データ配信システムのセキュリティを向上させることができる。

【0262】ライセンス管理モジュール511は、受理したアクセス制限情報ACmによって再生回数が制限されているか否かを判別し、再生回数が制限されていないときステップS266へ移行し、再生回数が制限されているときステップS268へ移行する(ステップS264)。そして、再生回数が制限されていないとき、ライセンス管理モジュール511は、配信サーバ10から受信した暗号化コンテンツおよびライセンスを他の装置へ貸出するためのチェックアウト可能数を含むチェックアウト情報を生成する(ステップS266)。この場合、チェックアウトの初期値は「3」に設定される。また、再生回数が制限されているとき、ライセンス管理モジュール511は、暗号化コンテンツデータを他の装置へ貸出するためのチェックアウト可能数を「0」に設定してチェックアウト情報を生成する(ステップS268)。ステップS268は、チェックアウトすることで再生回数の管理ができないための処理である。

【0263】図20を参照して、ステップS266またはステップS268の後、ライセンス管理モジュール511は、認証データ{Kpm5//Cm5}Kpa1をバス2を介してライセンス管理デバイス520へ出力する(ステップS270)。ライセンス管理デバイス520

0では、ライセンス管理モジュール511から認証データ{Kpm5//Cm5}Kpa1を受信し、復号処理部5208は、認証データ認証データ{Kpm5//Cm5}Kpa1を受取って、認証データ認証データ{Kpm5//Cm5}Kpa1に基づいて、Kpa保持部5214からレベル1認証鍵Kpa1を受取り、受取ったレベル1認証鍵Kpa1によって認証データ{Kpm5//Cm5}Kpa1を復号する(ステップS271)。

10 【0264】コントローラ5220は、復号処理部5208における復号処理結果から、処理が正常に行なわれたか否か、すなわち、正規の機関でクラス公開暗号鍵Kpm5とクラス証明書Cm5との正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう(ステップS272)。正当な認証データであると判断された場合、コントローラ5220は、クラス公開暗号鍵Kpm5およびクラス証明書Cm5を承認し、受理する。そして、次の処理(ステップS273)へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵Kpm5およびクラス証明書Cm5を受理しないで処理を終了する(ステップS298)。

20 【0265】認証の結果、正規の認証データを受信したことが認識されると、コントローラ5220は、次に、ライセンス管理モジュール511のクラス証明書Cm5が禁止クラスリストCRLにリストアップされているかどうかをメモリ5215のCRL領域5215Aに照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここで配信セッションを終了する(ステップS298)。

30 【0266】一方、ライセンス管理モジュール511のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する(ステップS273)。

【0267】認証の結果、正当な認証データを持つライセンス管理デバイスを備えるライセンス管理モジュール511からのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、ライセンス管理デバイス520において、セッションキー発生部5208は、セッションキーKs2aを生成し(ステップS274)、暗号処理部5210は、セッションキーKs2aをクラス公開暗号鍵Kpm5によって暗号化して暗号化データ{Ks2a}Km5を出力する(ステップS275)。

40 【0268】コントローラ5220は、暗号化データ{Ks2a}Km5をバスBS5、インタフェース5224、および端子5226を介して出力し、ライセンス管理モジュール511は、バスBS2を介して暗号化データ{Ks2a}Km5を受信し、クラス秘密復号鍵Kcm5によって暗号化データ{Ks2a}Km5を復号してセッションキーKs2aを受理する(ステップS27

6)。そして、ライセンス管理モジュール511は、セッションキーKs2bを生成し(ステップS277)、セッションキーKs2bをセッションキーKs2aによって暗号化して暗号化データ{Ks2b}Ks2aをバスBS2を介してライセンス管理デバイス520へ出力する(ステップS278)。

【0269】ライセンス管理デバイス520のコントローラ5220は、端子5226、インタフェース5224、およびバスBS5を介して暗号化データ{Ks2b}Ks2aを受け、復号処理部5212は、セッションキー発生部5208から出力されるセッションキーKs2aによって暗号化データ{Ks2b}Ks2aを復号してセッションキーKs2bを受理する(ステップS279)。そうすると、ライセンス管理モジュール511は、エントリ番号「0」をライセンス管理デバイス520へ入力し(ステップS280)、ライセンス管理デバイス520のコントローラ5220は、端子5226、インタフェース5224、およびバスBS5を介してエントリ番号「0」を受取る。そして、コントローラ5220は、メモリ5215のライセンス領域5215Bのうち、エントリ番号「0」によって指定されている領域に格納されているバイディングライセンス(トランザクションIDb、コンテンツIDb、バイディング鍵Kb、および制御情報ACmb、ACpb)を取得する(ステップS281)。そして、コントローラ5220は、制御情報ACmbに基づいてバイディングライセンスが有効か否かを判別し、有効でない場合、ステップS298へ移行し、配信セッションが終了する。ここで、有効な場合とは、制御情報ACmb内の再生回数が0でないこと、かつ、レベル1認証鍵KPa1によって認証された処理であるため制御情報ACmbのセキュリティレベルがレベル1であることを意味する。

【0270】一方、バイディングライセンスが有効な場合、ステップS283へ移行する(ステップS282)。

【0271】ステップS282において、バイディングライセンスが有効と判断されると、暗号処理部5206は、切換スイッチ5246を介して取得したバイディング鍵Kbおよび制御情報ACpbを、復号処理部5212によって復号され、スイッチ5242を介して取得したセッションキーKs2bによって暗号化して暗号化データ{Kb/ACpb}Ks2bを出力する(ステップS283)。

【0272】図21を参照して、コントローラ5220は、暗号化データ{Kb/ACpb}Ks2bをバスBS5、インタフェース5224、および端子5226を介して出力し、ライセンス管理モジュール511は、バスBS2を介して暗号化データ{Kb/ACpb}Ks2bを受信し、セッションキーKs2bによって暗号化データ{Kb/ACpb}Ks2bを復号してバ

ィング鍵Kbおよび制御情報ACpbを取得する(ステップS284)。

【0273】ステップS270からステップS284の一連の処理はバイディング鍵Kbをライセンス管理デバイス520から取得する処理であり、「バイディング鍵取得処理」と総称する。

【0274】そして、ライセンス管理モジュール511は、バスBS2を介してHDD530から暗号化機密ファイル160を取得し、その取得した暗号化機密ファイル160をバイディング鍵Kbによって復号して平文の機密ファイルを取得する(ステップS285)。そうすると、ライセンス管理モジュール511は、配信サーバ10から受理したライセンス(トランザクションID、コンテンツID、ライセンス鍵Kc、アクセス制限情報ACm、および再生期限ACp)とステップS266またはステップS268において生成されたチェックアウト情報とを機密情報nとして平文の機密ファイルに追記する(ステップS286)。その後、ライセンス管理モジュール511は、平文の機密ファイルをバイディング鍵Kbによって再び暗号化し、その暗号化した暗号化機密ファイル160によってHDD530に記録された暗号化機密ファイル160を更新する(ステップS287)。ライセンスを暗号化機密ファイル160に格納した後、ライセンス管理モジュール511は、配信サーバ10から送られたトランザクションIDと、暗号化コンテンツデータの配信要求を配信サーバ10へ送信する(ステップS288)。

【0275】配信サーバ10は、トランザクションIDおよび暗号化コンテンツデータの配信要求を受信し(ステップS289)、情報データベース304より、暗号化コンテンツデータ{Dc}Kcおよび付加情報Dc-infを取得して、これらのデータをバスBS1および通信装置350を介して出力する(ステップS290)。

【0276】ライセンス管理モジュール511は、{Dc}Kc/Dc-infを受信して、暗号化コンテンツデータ{Dc}Kcおよび付加情報Dc-infを受理する(ステップS291)。そして、ライセンス管理モジュール511は、暗号化コンテンツデータ{Dc}Kcおよび付加情報Dc-infをバスBS2を介してコンテンツファイルとしてハードディスク(HDD)530に記録する(ステップS292)。また、ライセンス管理モジュール511は、暗号化機密ファイル160に格納した機密情報nの機密情報番号nと、平文のトランザクションIDおよびコンテンツIDとを含むコンテンツファイル(暗号化コンテンツデータ{Dc}Kcと付加情報Dc-inf)に対応するライセンス管理ファイルを生成し、バスBS2を介してHDD530に記録する(ステップS293)。さらに、ライセンス管理モジュール511は、HDD530に記録されているコン

テンツリストファイルに受理したコンテンツ情報として、記録したコンテンツファイルおよびライセンス管理ファイルの名称や、付加情報Dc-infから抽出した暗号化コンテンツデータに関する情報(曲名、アーティスト名)等を追記し(ステップS294)、トランザクションIDと配信受理を配信サーバ10へ送信する(ステップS295)。

【0277】配信サーバ10は、トランザクションID//配信受理を受信すると(ステップS296)、課金データベース302への課金データの格納、およびトランザクションIDの配信記録データベース308への記録が行なわれて配信終了の処理が実行され(ステップS297)、全体の処理が終了する(ステップS298)。

【0278】このように、ライセンス管理モジュール511は、配信サーバ10との間でソフトウェアによってデータのやり取りを行ない、暗号化コンテンツデータおよびライセンスをソフト的に配信サーバ10から受信する。また、受信した暗号化コンテンツデータをHDD530に記録し、ライセンスを機密情報nとして機密ファイルに書き込み、その機密ファイルをバイディング鍵Kbによって暗号化して暗号化機密ファイル160にライセンスを格納する。そして、暗号化機密ファイル160を復号するバイディング鍵Kbはライセンス管理デバイス520に保持される。したがって、ライセンス管理モジュール511による暗号化コンテンツデータおよびライセンスの配信は、ライセンス管理デバイス520による暗号化コンテンツデータおよびライセンスの配信よりもセキュリティレベルは低い、記録管理においてはパーソナルコンピュータ50に関連付けていない点において、それに近いものになる。

【0279】[リッピング]パーソナルコンピュータ50のユーザは配信によって暗号化コンテンツとライセンスを取得するほかに、所有する音楽CDから、音楽データを取得して利用することが可能である。著作権者の権利保護の立場から音楽CDのデジタル複製は自由に行っているものではないが、個人が自己の使用目的のために、著作権保護機能を備えるツールを用いて複製し、音楽を楽しむことは許されている。そこで、ライセンス管理モジュール511は、音楽CDから音楽データを取得して、ライセンス管理モジュール511にて管理可能な暗号化コンテンツデータとライセンスを生成するリッピング機能を実現するプログラムも含んでいる。

【0280】また、近年の音楽CDには、音楽データ内に、ウォーターマークと呼ばれる電子すかしを挿入したものがあつる。このウォーターマークには、著作権者が利用者における利用の範囲が利用規則として書込まれている。利用規則が書込まれている音楽データからのリッピングでは、著作権保護の点から必ずこの利用規則に従う必要がある。以後、利用規則として、複製条件(複製禁

止/一代複製可/複製可」および最大チェックアウト数が記載されているとする。また、ウォーターマーク検出されない場合、すなわち、利用規則が書込まれていない従来の音楽CDであっても、著作権者の権利を保護するために、一代の複製ができ、最大チェックアウト数が「3」と解釈するものとする。

【0281】図22~図24を参照して、音楽データが記録された音楽CDからのリッピングによる暗号化コンテンツデータおよびライセンスの取得について説明する。

【0282】図22~図24は、音楽CDからリッピングによって暗号化コンテンツデータおよびライセンスを取得するための第1~第3のフローチャートである。

【0283】図22を参照して、リッピング動作が開始されると、CD-ROMドライブ540が音楽CDから検出した音楽データを取り込んで、取込んだ音楽データからウォーターマークによって記載された利用規則の検出が行なわれる(ステップS700)。そして、検出された利用規則に基づいて複製が可能か否かが判定される(ステップS701)。利用規則の複製条件が無制限の場合、ステップS203へ、複製条件が一代複製可の場合、ステップS702へ移行し、複製条件が複製禁止の場合、複製が禁止され、ステップS733へ移行してリッピング動作は終了する。さらに、装着されたCDにウォーターマークが含まれず、利用規則が得られない場合、ステップS705へ移行する。

【0284】ステップS701において、利用規則の複製条件が一代複製可の場合、ライセンス管理モジュール511は、取得した音楽データに含まれるウォーターマークを取得した利用規則の複製条件を複製禁止に変更したウォーターマークに付け替える(ステップS702)。そして、ステップS703へ移行する。複製ができる利用規則が検出された場合にステップS703において、ライセンス管理モジュール511は、利用規則を反映したアクセス制限情報ACmおよび再生期限ACpを生成する(ステップS703)。ここでも、複製条件に従い、複製可であれば、アクセス制限情報ACmの移動複製フラグを移動複製可(=3)に設定し、一代複製可であれば、リッピング自身が一代に当たるので移動複製禁止(=0)に設定する。また、対応する利用規則はないが再生回数は無制限、セキュリティレベルはレベル1に設定する。その後、ライセンス管理モジュール511は、利用規則の最大チェックアウト数を反映してチェックアウト可能数を設定する。最大チェックアウト数の指定がないときはチェックアウト可能数=3とする。そして、設定したチェックアウト可能数を含むチェックアウト情報を生成する(ステップS704)。

【0285】一方、ステップS701において、ウォーターマークが検出されず、利用規則が無いと判定された場合、ライセンス管理モジュール511は、アクセス制

限情報ACmの移動複製フラグを移動複製禁止(=0)、再生回数は無制限(=255)、セキュリティレベルは1に設定する。再生期限ACpは再生を無期限とする(ステップS705)。その後、ライセンス管理モジュール511は、初期値が3であるチェックアウト可能数を含むチェックアウト情報を生成する(ステップS706)。

【0286】ステップS704またはS706の後、ライセンス管理モジュール511は、乱数などによってライセンス鍵Kcを生成し(ステップS707)、ローカル使用のトランザクションIDおよびコンテンツIDを生成する(ステップS708)。次に、ライセンス管理モジュール511は、バインディング鍵取得処理を行う。図23のステップS709から図24のステップ723の一連の処理がバインディング鍵取得処理であり、配信2の配信処理における図20のステップS270から図21のステップS284の一連の処理と同じである。ゆえに、説明を省略する。

【0287】図24を参照して、バインディング鍵Kbを取得したライセンス管理モジュール511は、バスBS2を介してHDD530から暗号化機密ファイル160を取得し、その取得した暗号化機密ファイル160をバインディング鍵Kbによって復号して平文の機密ファイルを取得する(ステップS724)。そうすると、ライセンス管理モジュール511は、音楽CDから取得した音楽データを所定の方式に符号化してコンテンツデータDcを生成し(ステップS725)、コンテンツデータをライセンス鍵Kcによって暗号化して暗号化コンテンツデータ{Dc}Kcを生成する(ステップS726)。その後、ライセンス管理モジュール511は、キーボード560を介して入力されたユーザからの情報、および音楽CDからの情報に基づいて、コンテンツデータの付加情報Dc-infを生成し(ステップS727)、暗号化コンテンツデータ{Dc}Kcと付加情報Dc-infとをバスBS2を介してコンテンツファイルとしてHDD530に記録する(ステップS728)。

【0288】そうすると、ライセンス管理モジュール511は、生成したライセンス(トランザクションID、コンテンツID、ライセンス鍵Kc、アクセス制限情報ACm、および再生期限ACp)とステップS704またはステップS706において生成されたチェックアウト情報とを機密情報nとして平文の機密ファイルに追記する(ステップS729)。その後、ライセンス管理モジュール511は、平文の機密ファイルをバインディング鍵Kbによって暗号化し、その暗号化した暗号化機密ファイル160によってHDD530に記録された暗号化機密ファイル160を更新する(ステップS730)。ライセンスを暗号化機密ファイル160に格納した後、ライセンス管理モジュール511は、暗号化機密ファイル160に格納した機密情報nの機密情報番号n

と、平文のトランザクションIDおよびコンテンツIDとを含むコンテンツファイル(暗号化コンテンツデータ{Dc}Kcと付加情報Dc-inf)に対するライセンス管理ファイルを生成し、バスBS2を介してHDD530に記録する(ステップS731)。さらに、ライセンス管理モジュール511は、HDD530に記録されているコンテンツリストファイルに受理したコンテンツの情報として、記録したコンテンツファイル及びライセンス管理ファイルの名称や、付加情報Dc-infから抽出した暗号化コンテンツデータに関する情報(曲名、アーティスト名)等を追記し(ステップS732)、全体の処理が終了する(ステップS733)。

【0289】このように音楽CDからリッピングによっても暗号化コンテンツデータとライセンスとを取得できる。そして、音楽CDからのリッピングによって取得された暗号化コンテンツデータおよびライセンスは、配信によって取得された暗号化コンテンツデータおよびレベル1ライセンスと同じ方式によって、ライセンス管理モジュール511によって管理される。

【0290】図25を参照して、パーソナルコンピュータ50のライセンス管理モジュール511またはライセンス管理デバイス520によって受信された暗号化コンテンツデータおよびライセンスの管理について説明する。パーソナルコンピュータ50のHDD530は、コンテンツリストファイル150と、コンテンツリストファイル150は、コンテンツファイル1531~153nと、ライセンス管理ファイル1521~152nと、暗号化機密ファイルとを含む。

【0291】コンテンツリストファイル150は、所有するコンテンツの一覧形式のデータファイルであり、個々のコンテンツに対する情報(楽曲名、アーティスト名など)と、コンテンツファイルとライセンス管理ファイルを示す情報(ファイル名)などが含まれている。個々のコンテンツに対する情報は受信時に付加情報Dc-infから必要な情報を取得して自動的に、あるいは、ユーザの指示によって記載される。また、コンテンツファイルのみ、ライセンス管理ファイルのみの再生できないコンテンツについても一覧の中で管理することが可能である。

【0292】コンテンツファイル1531~153nは、ライセンス管理モジュール511またはライセンス管理デバイス520によって受信された暗号化コンテンツデータ{Dc}Kcと付加情報Dc-infとを記録するファイルであり、コンテンツごとに設けられる。

【0293】また、ライセンス管理ファイル1521~152nは、それぞれ、コンテンツファイル1531~153nに対応して記録されており、ライセンス管理モジュール511またはライセンス管理デバイス520によって受信されたライセンスを管理するためのファイルであり、ライセンスの格納場所を特定するための情報と

ライセンスに関する情報を含む。

【0294】格納場所を特定するための情報とは、ライセンス管理デバイス520にライセンスが記録された場合にはエントリ番号、もしくは暗号化機密ファイル内に記録された機密情報を特定する機密情報番号を言う。

【0295】ライセンスに関する情報とは、ライセンスを受信したときに平文にて参照できるトランザクションID、コンテンツIDや、ライセンス購入条件ACから容易に判断できるアクセス制限情報ACmおよび再生制御情報ACpにて制限されている事項の平文の写しである。これまで説明でも明らかなように、ライセンスは、コンテンツ保護のために参照することができないように保護され、記録されている。しかし、ライセンス鍵Kcを除く他の情報は、書き換えることさえできなければ、その内容が参照されてもコンテンツ保護の立場から何ら問題はない。アプリケーションプログラムにおいて、このライセンスに関する情報を参照して各処理を開始する。

【0296】暗号化機密情報ファイルは、ライセンス管理モジュール511にて管理されているライセンスやチェックアウト情報などを含む機密情報を含む。暗号化機密情報ファイルは、バインディング鍵Kbにて暗号化されている。

【0297】図25を参照して、具体的に説明する。ライセンス管理ファイル1521、1524は、それぞれ、エントリ番号1、mを含む。これは、ライセンス管理デバイス520によって受信され、ライセンス管理デバイス520のメモリ5215のライセンス領域5215Bにおいて管理されるライセンス(ライセンスID、ライセンス鍵Kc、アクセス制限情報ACmおよび再生

期限ACm)の管理領域を指定する番号である。  
 【0298】したがって、コンテンツファイル1531に記録されたファイル名の暗号化コンテンツデータを再生端末100に装着されたメモリカード110へ移動させるとき、コンテンツファイル1531~153nを検索してコンテンツファイル1531を抽出すれば、暗号化コンテンツデータを再生するライセンスがどこで管理されているかが解かる。コンテンツファイル1531に対応するライセンス管理ファイル1521に含まれるエントリ番号は「1」であるので、コンテンツファイル1531に記録されたファイル名の暗号化コンテンツデータを再生するライセンスは、ライセンス管理デバイス520のメモリ5215のライセンス領域5215Bのエントリ番号1によって指定された領域に記録されている。そうすると、HDD530に記録されたコンテンツリストファイル150のライセンス管理ファイル1521からエントリ番号1を讀出し、その讀出したエントリ番号1をライセンス管理デバイス520に入力することによって、メモリ5215のライセンス領域5215Bからライセンスを容易に取出し、メモリカード110へ

移動できる。そして、ライセンスを移動した後は、メモリ5215のライセンス領域5215Bにおいて指定されたエントリ番号1内のライセンスは削除されるので、それに対応してライセンス管理ファイル1523のように「ライセンス無」が記録される。

【0299】また、ライセンス管理モジュール511によって受信された暗号化コンテンツデータのライセンスを格納する機密情報は、ライセンス管理ファイル1522、1524、・・・、152nによって管理される。ライセンス管理ファイル1522、・・・、152nは、ライセンス管理モジュール511によって受信した暗号化コンテンツデータを再生するためのライセンスを格納する機密情報の機密情報番号を含む。

【0300】そうすると、たとえば、コンテンツファイル1532に記録されたファイル名の暗号化コンテンツデータをパーソナルコンピュータ80へ移動させるとき、コンテンツファイル1531~153nを検索してコンテンツファイル1532を抽出し、コンテンツファイル1532に対応するライセンス管理ファイル1522から機密情報番号1を取得する。一方、ライセンス管理デバイス520からバインディング鍵Kbを取得し、その取得したバインディング鍵Kbによって暗号化機密ファイル160を復号して平文の機密ファイルを取得する。そうすると、ライセンス管理ファイルから取得した機密情報番号1に対応する機密ファイル中の機密情報1に格納されているライセンスを取得することができる。

【0301】このように、本発明の実施の形態1においては、ライセンス管理モジュール511によって受信した暗号化コンテンツデータのライセンスは、暗号化機密ファイル160に機密情報nとして格納されており、暗号化機密ファイル160は、ライセンス管理デバイス520によってハード的に保持されたバインディング鍵Kbによってのみ復号可能である。つまり、バインディング鍵Kbは、暗号化コンテンツデータのライセンスを管理する共通鍵であり、バインディング鍵Kbがないとライセンスを取得することができない構造になっている。したがって、ライセンス管理モジュール511によって受信された暗号化コンテンツデータのライセンスは、暗号化機密ファイル160に書込まれてHDD530に記録されているため、実際はソフト的に管理されているが、ライセンス管理デバイス520に格納されたバインディング鍵Kbがないとライセンスを暗号化機密ファイル160から取出すことができないわけであるから、実質的には、ハードウェアによって管理されているに近い。

【0302】一方、ライセンス管理デバイス520によって受信されたライセンスは、メモリ5215のライセンス領域5215Bに格納されている。したがって、本発明の実施の形態1によって、ライセンス管理モジュール511によって受信されたライセンスの管理レベル

を、ライセンス管理デバイス520によって受信されたライセンスの管理レベルに近づけることができる。

【0303】なお、バイディングライセンスは、エントリ番号「0」に格納されている物としている。

【0304】〔移動1〕図1に示すデータ配信システムにおいて、配信サーバ10からパーソナルコンピュータ50のライセンス管理デバイス520へ配信された暗号化コンテンツデータおよびライセンスを再生端末100に装着されたメモリカード110へ送信する動作について説明する。なお、この動作を「移動1」という。移動は、セキュリティレベルがレベル2間でのみ行われる処理である図26～図29は、図1に示すデータ配信システムにおいて、ライセンス管理デバイス520が配信サーバ10から受信した暗号化コンテンツデータおよびライセンスを再生端末100に装着されたメモリカード110へ移動する移動動作を説明するための第1～第4のフローチャートである。

【0305】なお、図18における処理以前に、パーソナルコンピュータ50のユーザは、コンテンツリストファイルに従って、移動するコンテンツを決定し、HDD530のコンテンツファイルおよびライセンス管理ファイルが特定でき、メモリカード110の再生リストファイルを取得していることを前提として説明する。

【0306】図26を参照して、パーソナルコンピュータ50のキーボード560から移動リクエストが入力されると(ステップS300)、コントローラ510は、認証データの送信要求aをUSBインタフェース550、端子580、およびUSBケーブル70を介して再生端末100へ送信する(ステップS302)。そうすると、再生端末100のコントローラ1106は、端子1114、USBインタフェース1112およびバスBS3を介して認証データの送信要求を受信し、バスBS3およびメモリカードインタフェース1200を介して認証データの送信要求をメモリカード110へ送信する。そして、メモリカード110のコントローラ1420は、端子1426、インタフェース1424およびバスBS4を介して認証データの送信要求を受信する(ステップS304)。

【0307】コントローラ1420は、認証データの送信要求を受信すると、認証データ保持部1400から認証データ{K P m 3 / / C m 3} K P a 2をバスBS4を介して読出し、その読出した認証データ{K P m 3 / / C m 3} K P a 2をバスBS4、インタフェース1424および端子1426を介して再生端末100へ出力する。そして、再生端末100のコントローラ1106は、メモリカードインタフェース1200およびバスBS3を介して認証データ{K P m 3 / / C m 3} K P a 2を受取り、バスBS3、USBインタフェース1112、端子1114およびUSBケーブル70を介してパーソナルコンピュータ50へ認証データ{K P m 3 / /

C m 3} K P a 2を送信する(ステップS306)。

【0308】そうすると、パーソナルコンピュータ50のコントローラ510は、端子580およびUSBインタフェース550を介して認証データ{K P m 3 / / C m 3} K P a 2を受信し(ステップS308)、その受信した認証データ{K P m 3 / / C m 3} K P a 2をバスBS2を介してライセンス管理デバイス520へ送信する。ライセンス管理デバイス520のコントローラ5220は、端子5226、インタフェース5224、およびバスBS5を介して認証データ{K P m 3 / / C m 3} K P a 2を受信し、その受信した認証データ{K P m 3 / / C m 3} K P a 2を復号処理部5208へ与える。認証処理部5208は、K P a 保持部5214は、認証データ認証データ{K P m 3 / / C m 3} K P a 2を受取って、認証データ{K P m 3 / / C m 3} K P a 2に基づいて、K P a 保持部5214からレベル2認証鍵K P a 2を受取り、その受取ったレベル2認証鍵K P a 2によって認証データ{K P m 3 / / C m 3} K P a 2の復号処理を実行する(ステップS310)。コントローラ5220は、復号処理部5208における復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード110が正規のメモリカードからのクラス公開暗号鍵K P m 3とクラス証明書C m 3とを保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう(ステップS312)。正当な認証データであると判断された場合、コントローラ5220は、クラス公開暗号鍵K P m 3およびクラス証明書C m 3を承認し、受理する。そして、次の処理(ステップS314)へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵K P m 3およびクラス証明書C m 3を受理しないで処理を終了する(ステップS404)。

【0309】認証の結果、正規のメモリカードであることが認識されると、コントローラ5220は、次に、メモリカード110のクラス証明書C m 3が禁止クラスリストC R Lにリストアップされているかどうかをメモリ5215のC R L領域5215Aに照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここで移動動作を終了する(ステップS404)。

【0310】一方、メモリカード110のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する(ステップS314)。

【0311】認証の結果、正当な認証データを持つメモリカードを備える再生端末からのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、ライセンス管理デバイス520において、コントローラ5220は、移動を特定するための管理コードであるトランザクションIDをメモリ5215のライセンス

10

20

30

40

50



領域5215Bから取得する(ステップS316)。そして、セッションキー発生部5218は、移動のためのセッションキーKs22を生成する(ステップS318)。セッションキーKs22は、復号処理部5208によって得られたメモリカード110に対応するクラス公開暗号鍵Kpm3によって、暗号化処理部5210によって暗号化される(ステップS320)。コントローラ5220は、バスBS5を介して暗号化データ{Ks22}Km3を取得し、メモリ5215から取得したトランザクションIDを暗号化データ{Ks22}Km3に追加したトランザクションID/{Ks22}Km3をバスBS5、インタフェース5224および端子5226を介して出力する(ステップS322)。

【0312】図27を参照して、パーソナルコンピュータ50のコントローラ510は、バスBS2を介してトランザクションID/{Ks22}Km3を受信し(ステップS324)、USBインタフェース550、端子580、およびUSBケーブル70を介してトランザクションID/{Ks22}Km3を再生端末100へ送信する(ステップS324)。そうすると、再生端末100のコントローラ1106は、端子1114、USBインタフェース1112、およびBS3を介してトランザクションID/{Ks22}Km3を受信し、その受信したトランザクションID/{Ks22}Km3をメモリカードインタフェース1200を介してメモリカード110へ送信する。そして、メモリカード110のコントローラ1420は、端子1426、インタフェース1424およびバスBS4を介してトランザクションID/{Ks22}Km3を受信する(ステップS326)。復号処理部1422は、コントローラ1420からバスBS4を介して{Ks22}Km3を受取り、Km保持部1421からのクラス秘密復号鍵Km3によって{Ks22}Km3を復号してセッションキーKs22を受理する(ステップS328)。そして、セッションキー発生部1418は、セッションキーKs2を生成し(ステップS330)、コントローラ1420は、バスBS4を介してメモリ1415のCRL領域1415Aから禁止クラスリストの更新日時CRLdateを取得し、その取得した更新日時CRLdateを切換スイッチ1446へ与える(ステップS332)。

【0313】そうすると、暗号化処理部1406は、切換スイッチ1446の端子を順次切換えることによって取得したセッションキーKs2、個別公開暗号鍵Kpmc4および更新日時CRLdateを、復号処理部1404によって復号されたセッションキーKs22によって暗号化し、暗号化データ{Ks2//Kpmc4//CRLdate}Ks22を生成する。コントローラ1420は、暗号化データ{Ks2//Kpmc4//CRLdate}Ks22をバスBS4、インタフェース

1424および端子1426を介して再生端末100へ出力し、再生端末100のコントローラ1106は、メモリカードインタフェース1200を介して暗号化データ{Ks2//Kpmc4//CRLdate}Ks22を受取る。そして、コントローラ1106は、USBインタフェース1112、端子1114、およびUSBケーブル70を介してパーソナルコンピュータ50へ送信する(ステップS334)。

【0314】パーソナルコンピュータ50のコントローラ510は、端子580およびUSBインタフェース550を介して暗号化データ{Ks2//Kpmc4//CRLdate}Ks22を受信し(ステップS336)、バスBS2を介して暗号化データ{Ks2//Kpmc4//CRLdate}Ks22をライセンス管理デバイス520へ入力する(ステップS338)。ライセンス管理デバイス520のコントローラ5220は、端子5226、インタフェース5224およびバスBS5を介して暗号化データ{Ks2//Kpmc4//CRLdate}Ks22を受信し、その受信した暗号化データ{Ks2//Kpmc4//CRLdate}Ks22を復号処理部5212に与える。復号処理部5212は、セッションキー発生部5218からのセッションキーKs22によって暗号化データ{Ks2//Kpmc4//CRLdate}Ks22を復号し、セッションキーKs2、公開暗号鍵Kpmc4および禁止クラスリストCRLdateを受理する(ステップS340)。

【0315】そうすると、パーソナルコンピュータ50のコントローラ510は、ステップS324において、ライセンス管理ファイルに含まれるライセンスのエントリ番号をHDD530から読出す。そして、コントローラ510は、その読出したエントリ番号をバスBS2を介してライセンス管理デバイス520へ入力する(ステップS342)。ライセンス管理デバイス520のコントローラ5220は、端子5226、インタフェース5224、およびバスBS5を介してエントリ番号を受信し、メモリ5215のライセンス領域5215Bにおいて受信したエントリ番号によって指定された領域からライセンス(トランザクションID、コンテンツID、ライセンス鍵Kc、アクセス制限情報ACm、再生期限ACp)を読出す(ステップS344)。

【0316】アクセス制限情報ACmの受理に応じて、コントローラ5220は、アクセス制限情報ACmを確認する(ステップS346)。つまり、コントローラ5220は、取得したアクセス制限情報ACmのセキュリティレベル、再生回数、移動複製フラグについて順に判定を行う。最初に、アクセス制限情報ACmのセキュリティレベルとステップS310にて用いた認証鍵に基づいて、レベル1認証鍵Kpa1を利用し、かつ、アクセス制限情報ACmのセキュリティレベルが2の場合に

10

20

30

40

50

は、ライセンスの管理要求レベルより低いセキュリティレベルへ出力となるので、ステップS404へ移行し、移動動作を中止する。それ以外の場合には次の判定を行う。アクセス制限情報ACmの再生回数に基づいて、再生端末100に装着されたメモリカード110へ移動しようとするライセンスがアクセス制限情報ACmによって暗号化コンテンツデータの再生ができないライセンスになっていないか否かを確認する。再生回数がアクセス制限情報ACmによる制限回数に達している場合(=0)、暗号化コンテンツデータをライセンスによって再生することができず、その暗号化コンテンツデータとライセンスとを再生端末100に装着されたメモリカード110へ移動する意味がないからである。再生回数が「0」の場合に、ステップS404へ移行し、移動動作を中止する。それ以外(再生回数≠0)の場合には次の判定を行う。アクセス制限情報ACmの移動複製フラグに基づいて、移動複製禁止「=0」のときステップS404並行し、移動動作を中止する。移動のみ可のとき、ステップS348並行し、そして、コントローラ5220は、メモリ5215のライセンス領域5215Bにおいて指定されたエントリ番号内のライセンスを削除して(ステップS348)、ステップS350並行する。移動複製可「=2」のとき、ライセンスの複製であると判断され、ステップS348を行わずにステップS350並行。

【0317】図28を参照して、暗号化処理部5217は、復号処理部5212によって得られたライセンス管理デバイス520固有の個別公開暗号鍵Kpmc4によってライセンスを暗号化して暗号化データ{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4を生成する(ステップS350)。そして、メモリカード110から送信された更新日時CRLdateをライセンス管理デバイス520がCRL領域5215Aに保持している禁止クラスリストの更新日時と比較し、いずれの禁止クラスリストが新しいかが判断され、メモカード100の方が新しいと判断されたとき、ステップS352へ移行する。また、ライセンス管理デバイス520の方が新しいと判断されたときはステップS362へ移行する(ステップS352)。

【0318】データCRLdateが最新と判断されたとき、暗号化処理部5206は、暗号化処理部5217から出力された暗号化データ{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4をセッションキー発生部5218において発生されたセッションキーKs2によって暗号化を行い、暗号化データ{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2をバスBS5に出力する。そして、コントローラ5220は、バスBS5上の暗号化データ{トランザクションID//コンテンツID//Kc//ACm//ACp}K

mc4}Ks2をインタフェース5224および端子5226を介してパーソナルコンピュータ50へ送信する(ステップS354)。

【0319】パーソナルコンピュータ50のコントローラ510は、暗号化データ{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2を受取り、USBインタフェース550、端子580、およびUSBケーブル70を介して再生端末100へ送信する(ステップS356)。

【0320】再生端末100のコントローラ1106は、端子1114、USBインタフェース1112、およびバスBS3を介して暗号化データ{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2を受信し、その受信した暗号化データ{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2をバスBS3およびメモリカードインタフェース1200を介してメモリカード110へ送信する。そして、メモリカード110のコントローラ1420は、端子1426、端子1424、およびバスBS4を介して暗号化データ{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2を受信する(ステップS358)。

【0321】メモリカード110の復号処理部1412は、暗号化データ{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2をバスBS4を介して受取り、セッションキー発生部1418によって発生されたセッションキーKs2によって復号し、{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4を受理する(ステップS360)。その後、図29に示すステップS376へ移行する。

【0322】一方、ステップS350において、ライセンス管理デバイス520の方が新しいと判断されると、ライセンス管理デバイス520のコントローラ5220は、バスBS5を介してメモリ5215のCRL領域5215Aから最新の禁止クラスリストCRLを取得する(ステップS362)。

【0323】暗号化処理部5206は、暗号化処理部5217の出力と、コントローラ5220がバスBS5を介してメモリ5215から取得した禁止クラスリストのデータCRLとを、それぞれ、切換スイッチ5242および5246を介して受取り、セッションキー発生部5218において生成されたセッションキーKs2によって暗号化する。暗号化処理部5206より出力された暗号化データ{CRL//トランザクションID//コンテンツID//インタフェース5224、および端子5226を介してパーソナルコンピュータ50に出力される(ステップS364)。

【0324】パーソナルコンピュータ50のコントロー

ラ510は、出力された暗号化データ {CRL// {トランザクションID//コンテンツID//Kc//ACm//ACp} Kmc4} Ks2を受信し、USBインタフェース550、端子580、およびUSBケーブル70を介して暗号化データ {CRL// {トランザクションID//コンテンツID//Kc//ACm//ACp} Kmc4} Ks2を再生端末100へ送信する (ステップS368)。再生端末100のコントローラ1106は、端子1114、USBインタフェース1112、およびバスBS3を介して暗号化データ {CRL// {トランザクションID//コンテンツID//Kc//ACm//ACp} Kmc4} Ks2を受取り、バスBS3およびメモリカードインタフェース1200を介して暗号化データ {CRL// {トランザクションID//コンテンツID//Kc//ACm//ACp} Kmc4} Ks2をメモリカード110へ送信する。そして、メモリカード110のコントローラ1420は、端子1426、インタフェース1424、およびバスBS4を介して暗号化データ {CRL// {トランザクションID//コンテンツID//Kc//ACm//ACp} Kmc4} Ks2を受信する (ステップS370)。

【0325】メモリカード110において、復号処理部1412は、セッションキー発生部1418から与えられたセッションキーKs2を用いてバスBS4上の受信データを復号し、CRLと {トランザクションID//コンテンツID//Kc//ACm//ACp} Kmc4とを受信する (ステップS372)。コントローラ1420は、復号処理部1412によって受信されたデータCRLをバスBS4を介して受取り、その受取ったデータCRLによってメモリ1415のCRL領域1415Aを書換える (ステップS374)。

【0326】ステップS354、S356、S358、S360は、送信側のメモリカード110の禁止クラスリストCRLが、受信側のライセンス管理デバイス520の禁止クラスリストCRLより、新しい場合のライセンス鍵Kc等のメモリカード110への移動動作であり、ステップS362、S364、S368、S370、S372、S374は、送信側のライセンス管理デバイス520の禁止クラスリストCRLが、受信側のメモリカード110の禁止クラスリストCRLより、新しい場合のライセンス鍵Kc等のメモリカード110への移動動作である。このように、メモリカード110から送られてきた禁止クラスリストの更新日時CRLdateによって、逐一、確認し、より最新の禁止クラスリストCRLをメモリカード110の禁止クラスリストCRLとしてCRL領域1514Aに格納させることによって、クラス秘密鍵が漏洩などのセキュリティ機能の破られた機器へのライセンスの流出を防止できる。

【0327】図29を参照して、ステップS360また

はステップS374の後、コントローラ1420の指示によって、暗号化ライセンス {トランザクションID//コンテンツID//Kc//ACm//ACp} Kmc4は、復号処理部1404において、個別秘密復号鍵Kmc4によって復号され、ライセンス (ライセンス鍵Kc、トランザクションID、コンテンツID、アクセス制限情報ACmおよび再生期限ACp) が受理される (ステップS376)。

【0328】このように、ライセンス管理デバイスおよびメモリカードでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、暗号化コンテンツデータおよびライセンスの移動動作におけるセキュリティを向上させることができる。

【0329】パーソナルコンピュータ50のコントローラ510は、メモリカード110へ移動したライセンスを格納するためのエントリ番号を、USBインタフェース550、端子580、およびUSBケーブル70を介して再生端末100へ送信する (ステップS378)。そうすると、再生端末100のコントローラ1106は、端子1114、USBインタフェース1112、およびバスBS3を介してエントリ番号を受取り、バスBS3およびメモリカードインタフェース1200を介してメモリカード110へ送信し、メモリカード110のコントローラ1420は、端子1426およびインタフェース1424を介してエントリ番号を受取り、その受取ったエントリ番号によって指定されるメモリ1415のライセンス領域1415Bに、ステップS376において取得したライセンス (ライセンス鍵Kc、トランザクションID、コンテンツID、アクセス制限情報ACmおよび再生期限ACp) を格納する (ステップS380)。

【0330】パーソナルコンピュータ50のコントローラ510は、メモリカード110のメモリ1415に格納されたライセンスのエントリ番号と、平文のトランザクションIDおよびコンテンツIDを含むメモリカード110へ移動しようとする暗号化コンテンツデータ {Dc} Kcと付加情報Dc-infに対するライセンス管理ファイルを生成し、メモリカード110へ送信する (ステップS382)。

【0331】メモリカード110のコントローラ1420は、再生端末100を介してライセンス管理ファイルを受信し、メモリ1415のデータ領域1415Cに受信したライセンス管理ファイルを記録する (ステップS384)。

【0332】そして、パーソナルコンピュータ50のコントローラ510は、ステップS346の判断に従って、移動であればステップS388へ移行し、複製であ

10

20

30

40

50

ればステップS388を行なわないで、ステップS390並行する(ステップS386)。そして、移動の場合、HDD530に記録されたライセンスのうち、メモリカード110へ移動したライセンスに対するライセンス管理ファイルのライセンスエントリ番号を、ライセンス無に更新する(ステップS386)。

【0333】その後、コントローラ510は、メモリカード110へ移動しようとするコンテンツファイル(暗号化コンテンツデータ{Dc}Kcと付加情報Dc-inf)とをHDD530から取得し、{Dc}Kc/Dc-infをメモリカード110へ送信する(ステップS390)。メモリカード110のコントローラ1420は、再生端末100を介して{Dc}Kc/Dc-infを受信し(ステップS392)、バスBS4を介して受信した{Dc}Kc/Dc-infをコンテンツファイルとしてメモリ1415のデータ領域1415Cに記録する(ステップS394)。

【0334】そうすると、パーソナルコンピュータ50のコントローラ510は、メモリカード110へ移動した楽曲を追記した再生リストファイルを作成し(ステップS396)、再生リストファイルと、再生リストファイルの書換指示とをメモリカード110へ送信する(ステップS398)。メモリカード110のコントローラ1420は、再生端末100を介して再生リストファイルと書換指示とを受信し(ステップS400)、バスBS4を介してメモリ1415のデータ領域1415Cに記録されている再生リストファイルを受信した再生リストファイルに書換え(ステップS402)、移動動作が終了する(ステップS404)。

【0335】なお、再生リストファイルとは、HDDに記録されていたコンテンツリストファイルと、同じ目的で作られた再生端末用の管理情報ファイルである。再生端末100は、この再生リストファイルに含まれるコンテンツの登場順に、コンテンツファイルおよびライセンス管理ファイルを特定して再生を行なう。

【0336】このようにして、再生端末100に装着されたメモリカード110が正規の機器であること、同時に、クラス証明書Cm3とともに暗号化して送信できた公開暗号鍵Kpm3が有効であることを確認した上で、クラス証明書Cm3が禁止クラスリスト、すなわち、公開暗号鍵Kpm3による暗号化が破られたクラス証明書リストに記載されていないメモリカードへの移動要求に対してのみコンテンツデータを移動することができ、不正なメモリカードへの移動および解読されたクラス鍵を用いた移動を禁止することができる。また、この移動動作を用いることによって、配信サーバ10との通信機能を有さない再生端末102のユーザも、パーソナルコンピュータ50を介して暗号化コンテンツデータおよびライセンスをメモリカードに受信することができ、ユーザの利便性は向上する。

【0337】また、説明から明らかなように移動処理として説明したが、コンテンツ供給者によって、ライセンスの複製が許可されている場合には、複製処理として実行され、送信側のライセンス管理デバイス511にライセンスはそのまま保持される。この場合の複製は、配信時にコンテンツ供給者、すなわち、著作権所有者が複製を許可し、アクセス制限情報ACmの移動複製フラグを移動複製可に設定した場合にのみ許可される行為で合え居、著作権所有者の権利を阻害した行為ではない。アクセス制限情報はライセンスの一部であり、その機密性は保証されているので、著作権は保護されている。

【0338】なお、上記においては、パーソナルコンピュータ50のライセンス管理デバイス520からメモリカード110へのライセンスの移動について説明したが、メモリカード110からライセンス管理デバイス520へのライセンスの移動も、図26～図29に示すフローチャートに従って行なわれる。また、パーソナルコンピュータ50が配信サーバ10から受信した暗号化コンテンツデータおよびライセンスをメモリカード110へ移動できるのでは、ライセンス管理デバイス520が配信サーバ10からハード的に受信した暗号化コンテンツデータおよびライセンスであり、ライセンス管理モジュール511が配信サーバ10からソフト的に受信した暗号化コンテンツデータおよびライセンスを「移動」という概念によってメモリカードへ送信することはできない。ライセンス管理モジュール511は、ライセンス管理デバイス520よりも低いセキュリティレベルによってソフト的に配信サーバ10との間で認証データおよび暗号鍵等のやり取りを行ない、暗号化コンテンツデータおよびライセンスを受信するので、その受信動作において暗号化が破られる可能性は、ライセンス管理デバイス520によって暗号化コンテンツデータおよびライセンスを受信する場合よりも高い。したがって、低いセキュリティレベルによって受信し、かつ、管理された暗号化コンテンツデータおよびライセンスを、ライセンス管理デバイス520と同じセキュリティレベルによって暗号化コンテンツデータおよびライセンスを受信して管理するメモリカード110へ「移動」という概念によって自由に移すことができるとすると、メモリカード110におけるセキュリティレベルが低下するので、これを防止するためにライセンス管理モジュール511によって受信した暗号化コンテンツデータおよびライセンスを「移動」という概念によってメモリカード110へ送信できなくしたものである。

【0339】しかしながら、ライセンス管理モジュール511によって受信されたセキュリティレベルの低い暗号化コンテンツデータおよびライセンスを、一切、メモリカード110へ移すことができないとすると、著作権を保護しながらコンテンツデータの自由なコピーを許容するデータ配信システムの趣旨に反し、ユーザの利便性

も向上しない。そこで、次に説明するチェックアウトおよびチェックインの概念によってライセンス管理モジュール511によって受信した暗号化コンテンツデータおよびライセンスをメモリカード110へ送信できるようにした。

【0340】[チェックアウト] 図1に示すデータ配信システムにおいて、配信サーバ10からパーソナルコンピュータ50のライセンス管理モジュール511へ配信された暗号化コンテンツデータおよびライセンスを再生端末100に装着されたメモリカード110に送信する動作について説明する。なお、この動作を「チェックアウト」という。

【0341】図30～図34は、図1に示すデータ配信システムにおいて、ライセンス管理モジュール511が配信サーバ10から受信した暗号化コンテンツデータおよびライセンスを、返却を条件として再生端末100に装着されたメモリカード110へ貸出すチェックアウト動作を説明するための第1～第5のフローチャートである。なお、図30における処理以前に、パーソナルコンピュータ50のユーザは、コンテンツリストファイルに従って、チェックアウトするコンテンツを決定し、HDD530のコンテンツファイルおよびライセンス管理ファイルが特定でき、メモリカード110の再生リストファイルを取得していていることを前提として説明する。

【0342】図30を参照して、パーソナルコンピュータ50のキーボード560からチェックアウトリクエストが入力されると(ステップS500)、ライセンス管理モジュール511は、バインディング鍵取得処理を行う。図30のステップS501から図31のステップ515の一連の処理がバインディング鍵取得処理であり、配信2のフローチャートにおける図20のステップS270から図21のステップS284の一連の処理と同じである。ゆえに、説明を省略する。

【0343】バインディング鍵Kbを取得したライセンス管理モジュール511は、バスBS2を介してHDD530から暗号化機密ファイル160を取得し、その取得した暗号化機密ファイル160をバインディング鍵Kbによって復号して平文の機密ファイルを取得する(ステップS516)。その後、ライセンス管理モジュール511は、ライセンス管理ファイルに記録された機密情報番号nに対応する機密ファイル内の機密情報n(トランザクションID、コンテンツID、ライセンス鍵Kc、アクセス制限情報ACm、再生期限ACp、およびチェックアウト情報)を取得する(ステップS517)。

【0344】そうすると、ライセンス管理モジュール511は、取得したアクセス制限情報ACmに基づいてライセンスがチェックアウト可能か否かを確認する(ステップS518)、つまり、ライセンス管理モジュール511は、再生端末100に装着されたメモリカード11

0へチェックアウトしようとするライセンスがアクセス制限情報ACmの再生回数によって暗号化コンテンツデータの再生回数の制限がないか、再生ができないライセンスになっていないか否かを確認する。再生回数に制限がある場合、暗号化コンテンツデータおよびライセンスをチェックアウトしない。

【0345】ステップS518において、再生に制限がある場合、ステップS564へ移行し、チェックアウト動作は終了する。ステップS518において、暗号化コンテンツデータの再生回数がアクセス制限情報ACmによる制限回数に達していない場合、ステップS519へ移行する。そして、ライセンス管理モジュール511は、取得したチェックアウト情報に含まれるチェックアウト可能数が「0」よりも大きいか否かを確認する(ステップS519)。ステップS519において、チェックアウト可能数が「0」であれば、チェックアウトできるライセンスが無いので、ステップS564へ移行し、チェックアウト動作は終了する。ステップS519において、チェックアウト可能数が「0」よりも大きいとき、ライセンス管理モジュール511は、USBインタフェース550、端子580、およびUSBケーブル70を介して認証データの送信要求を送信する(ステップS520)。再生端末100のコントローラ1106は、端子1114、USBインタフェース1112、およびバスBS3を介して認証データの送信要求を受信し、その受信した認証データの送信要求をバスBS3およびメモリカードインタフェース1200を介してメモリカード110へ送信する。そして、メモリカード110のコントローラ1420は、端子1426、インタフェース1424およびバスBS4を介して認証データの送信要求を受信する(ステップS521)。

【0346】コントローラ1420は、認証データの送信要求を受信すると、認証データ保持部1400から認証データ{Kp m3//Cm3} KPa2をバスBS4を介して読出し、その読出した認証データ{Kp m3//Cm3} KPa2をバスBS4、インタフェース1424および端子1426を介して再生端末100へ出力する。そして、再生端末100のコントローラ1106は、メモリカードインタフェース1200およびバスBS3を介して認証データ{Kp m3//Cm3} KPa2を受取り、バスBS3、USBインタフェース1112、端子1114およびUSBケーブル70を介してパーソナルコンピュータ50へ認証データ{Kp m3//Cm3} KPa2を送信する(ステップS522)。

【0347】そうすると、パーソナルコンピュータ50のライセンス管理モジュール511は、端子580およびUSBインタフェース550を介して認証データ{Kp m3//Cm3} KPa2を受信し(ステップS523)、その受信した認証データ{Kp m3//Cm3} KPa2をレベル2認証鍵KPa2によって復号する

10

20

30

40

50

(ステップS524)。

【0348】図32を参照して、ライセンス管理モジュール511は、復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード110が正規のメモリカードからのクラス公開暗号鍵K P m 3とクラス証明書C m 3とを保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう(ステップS525)。正当な認証データであると判断された場合、ライセンス管理モジュール511は、クラス公開暗号鍵K P m 3およびクラス証明書C m 3を承認し、

10 受理する。そして、次の処理(ステップS526)へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵K P m 3およびクラス証明書C m 3を受信しないで処理を終了する(ステップS564)。

【0349】認証の結果、正規のメモリカードであることが認識されると、ライセンス管理モジュール511は、次に、メモリカード110のクラス証明書C m 3が禁止クラスリストC R LにリストアップされているかどうかをH D D 5 3 0に照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここでチェックアウト動作を終了する(ステップS564)。一方、メモリカード110のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する(ステップS526)。

【0350】認証の結果、正当な認証データを持つメモリカードを備える再生端末からのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、ライセンス管理モジュール511は、チェックアウトを特定するための管理コードであるチェックアウト用

30 トランザクションIDを、メモリカード110の格納されている全てのトランザクションIDと異なる値をとり、かつ、ローカル使用のトランザクションIDとして生成する。生成する(ステップS527)。そして、ライセンス管理モジュール511は、チェックアウトのためのセッションキーK s 2 bを生成し(ステップS528)、メモリカード110から送信されたクラス公開暗号鍵K P m 3によって、生成したセッションキーK s 2 bを暗号化する(ステップS529)。そして、ライ

40 センス管理モジュール511は、暗号化データ{K s 2 b} K m 3にチェックアウト用トランザクションIDを追加したチェックアウト用トランザクションID//{K s 2 b} K m 3をUSBインタフェース550、端子580、およびUSBケーブル70を介して再生端末100へ送信する(ステップS530)。そうすると、再生端末100のコントローラ1106は、端子1114、USBインタフェース1112、およびバスBS3を介してチェックアウト用トランザクションID//{K s 2 b} K m 3を受信し、その受信したチェックア

ウト用トランザクションID//{K s 2 b} K m 3をメモリカードインタフェース1200を介してメモリカード110へ送信する。そして、メモリカード110のコントローラ1420は、端子1426、インタフェース1424およびバスBS4を介してチェックアウト用トランザクションID//{K s 2 b} K m 3を受信する(ステップS531)。復号処理部1422は、コントローラ1420からバスBS4を介して{K s 2 b} K m 3を受取り、K m保持部1421からの秘密復号鍵K m 3によって{K s 2 b} K m 3を復号してセッションキーK s 2 bを受理する(ステップS532)。そして、セッションキー発生部1418は、セッションキーK s 2 cを生成し(ステップS533)、コントローラ1420は、バスBS4を介してメモリ1415のC R L領域1415Aから禁止クラスリストの更新日時C R L d a t eを取得し、その取得した更新日時C R L d a t eを切

50 換スイッチ1446へ与える(ステップS534)。

【0351】そうすると、暗号化処理部1406は、切換スイッチ1446の端子を順次切換えることによって取得したセッションキーK s 2 c、個別公開暗号鍵K P m c 4および更新日時C R L d a t eを、復号処理部1404によって復号されたセッションキーK s 2 bによって暗号化し、暗号化データ{K s 2 c//K P m c 4//C R L d a t e} K s 2 bを生成する。コントローラ1420は、暗号化データ{K s 2 c//K P m c 4//C R L d a t e} K s 2 bをバスBS4、インタフェース1424および端子1426を介して再生端末100へ出力し、再生端末100のコントローラ1106は、メモリカードインタフェース1200を介して暗号化データ{K s 2 c//K P m c 4//C R L d a t e} K s 2 bを受取る。そして、コントローラ1106は、USBインタフェース1112、端子1114、およびUSBケーブル70を介してパーソナルコンピュータ50へ送信する(ステップS535)。

【0352】パーソナルコンピュータ50のライセンス管理モジュール511は、端子580およびUSBインタフェース550を介して暗号化データ{K s 2 c//K P m c 4//C R L d a t e} K s 2 bを受信し(ステップS536)、その受信した暗号化データ{K s 2 c//K P m c 4//C R L d a t e} K s 2 bをセッションキーK s 2 bによって復号し、セッションキーK s 2 c、個別公開暗号鍵K P m c 4および更新日時C R L d a t eを受理する(ステップS537)。そして、ライセンス管理モジュール511は、再生端末100に装着されたメモリカードから他のメモリカード等へライセンスが移動/複製されるのを禁止したチェックアウト用アクセス制限情報A C mを生成する。すなわち、再生回数を無制限(=255)、移動複製フラグを移動複製不可(=3)、セキュリティレベルを1に設定したアク

セス制限情報ACmを生成する(ステップS538)。【0353】図33を参照して、ライセンス管理モジュール511は、ステップS537において受信したメモリカード110に固有の公開暗号鍵Kpmc4によってライセンスを暗号化して暗号化データ(チェックアウト用トランザクションID//コンテンツID//Kc//チェックアウト用ACm//ACp)Kmc4を生成する(ステップS539)。そして、メモリカード110から送信された更新日時CRLdateが、ライセンス管理モジュール511が管理するHDD530に保持される禁止クラスリストの更新日時と比較し、いずれの禁止クラスリストが新しいかが判断され、メモリカード110の方が新しいと判断されたとき、ステップS541へ移行する。また、逆に、ライセンス管理モジュール511の方が新しいと判断されたときはステップS544へ移行する(ステップS540)。

【0354】メモリカード110の方が新しいと判断されたとき、ライセンス管理モジュール511は、暗号化データ(チェックアウト用トランザクションID//コンテンツID//Kc//チェックアウト用ACm//ACp)Kmc4をセッションキーKs2cによって暗号化を行い、暗号化データ{(チェックアウト用トランザクションID//コンテンツID//Kc//チェックアウト用ACm//ACp)Kmc4)Ks2cをUSBインタフェース550、端子580、およびUSBケーブル70を介して再生端末100へ送信する(ステップS541)。

【0355】再生端末100のコントローラ1106は、端子1114、USBインタフェース1112、およびバスBS3を介して暗号化データ{(チェックアウト用トランザクションID//コンテンツID//Kc//チェックアウト用ACm//ACp)Kmc4)Ks2cを受信し、その受信した暗号化データ{(チェックアウト用トランザクションID//コンテンツID//Kc//チェックアウト用ACm//ACp)Kmc4)Ks2cをバスBS3およびメモリカードインタフェース1200を介してメモリカード110へ送信する。そして、メモリカード110のコントローラ1420は、端子1426、端子1424、およびバスBS4を介して暗号化データ{(チェックアウト用トランザクションID//コンテンツID//Kc//チェックアウト用ACm//ACp)Kmc4)Ks2cを受信する(ステップS542)。

【0356】メモリカード110の復号処理部1412は、暗号化データ{(チェックアウト用トランザクションID//コンテンツID//Kc//チェックアウト用ACm//ACp)Kmc4)Ks2cをバスBS4を介して受取り、セッションキー発生部1418によって発生されたセッションキーKs2cによって復号し、(チェックアウト用トランザクションID//コンテン

ツID//Kc//チェックアウト用ACm//ACp)Kmc4を受信する(ステップS543)。その後、図34に示すステップS549へ移行する。

【0357】一方、ステップS540において、ライセンス管理モジュール511の禁止クラスリストのほうが新しいと判断されると、ライセンス管理モジュール511は、HDD530からライセンス管理モジュール511の管理する禁止クラスリストCRLを取得する(ステップS544)。

【0358】そして、ライセンス管理モジュール511は、(チェックアウト用トランザクションID//コンテンツID//Kc//チェックアウト用ACm//ACp)Kmc4と、HDD530から取得した禁止クラスリストのデータCRLとをセッションキーKs2cによって暗号化し、その暗号化データ{CRL// (チェックアウト用トランザクションID//コンテンツID//Kc//チェックアウト用ACm//ACp)Kmc4)Ks2cをUSBインタフェース550、端子580およびUSBケーブル70を介して再生端末100へ送信する(ステップS545)。再生端末100のコントローラ1106は、端子1114、USBインタフェース1112、およびバスBS3を介して暗号化データ{CRL// (チェックアウト用トランザクションID//コンテンツID//Kc//チェックアウト用ACm//ACp)Kmc4)Ks2cを受信し、その受信した暗号化データ{CRL// (チェックアウト用トランザクションID//コンテンツID//Kc//チェックアウト用ACm//ACp)Kmc4)Ks2cをバスBS3およびメモリカードインタフェース1200を介してメモリカード110へ出力する。そうすると、メモリカード110のコントローラ1420は、端子1426、インタフェース1424、およびバスBS4を介して暗号化データ{CRL// (チェックアウト用トランザクションID//コンテンツID//Kc//チェックアウト用ACm//ACp)Kmc4)Ks2cを受信する(ステップS546)。

【0359】メモリカード110において、復号処理部1412は、セッションキー発生部1418から与えられたセッションキーKs2cを用いてバスBS4上の受信データを復号し、CRLと(チェックアウト用トランザクションID//コンテンツID//Kc//チェックアウト用ACm//ACp)Kmc4とを受信する(ステップS547)。コントローラ1420は、復号処理部1412によって受理されたデータCRLをバスBS4を介して受取り、その受取ったデータCRLによってメモリ1415のCRL領域1415Aを書換える(ステップS548)。

【0360】ステップS541、S542、S543は、送信側のライセンス管理モジュール511の禁止クラスリストCRLより、受信側のメモリカード110の

禁止クラスリストCRLが新しい場合のライセンス鍵Kc等のメモリカード110へのチェックアウト動作であり、ステップS544、S545、S546、S547、S548は、受信側のメモリカード110の禁止クラスリストCRLより、送信側のライセンス管理モジュール511の禁止クラスリストCRLが新しい場合のライセンス鍵Kc等のメモリカード110へのチェックアウト動作である。このように、メモリカード110へライセンスを送信するときに、メモリカード100がCRL領域1415Bで保持する禁止クラスリストCRLより、HDD530に新しい禁止クラスリストCRLが記録されている場合には禁止クラスリストCRLをHDD530から取得し、禁止クラスリストCRLをメモリカード110に配信することによって、メモリカード100がCRL領域1415Bで保持する禁止クラスリストを更新していくことができる、クラス鍵が破られたメモリカード110へのらい線への送信を禁止することができる、配信されたライセンスの流出を防止できる。

【0361】図34を参照して、ステップS543またはステップS548の後、コントローラ1420の指示によって、暗号化ライセンス{チェックアウト用トランザクションID//コンテンツID//Kc//チェックアウト用ACm//ACp}Kmc4は、復号処理部1404において、秘密復号鍵Kmc4によって復号され、ライセンス(ライセンス鍵Kc、チェックアウト用トランザクションID、コンテンツID、チェックアウト用ACmおよび再生期限ACp)が受理される(ステップS549)。

【0362】そして、パーソナルコンピュータ50のライセンス管理モジュール511は、メモリカード110へチェックアウトしたライセンスを格納するためのエン트리番号を、USBインタフェース550、端子580、およびUSBケーブル70を介して再生端末102へ送信しする(ステップS550)。そうすると、再生端末102のコントローラ1106は、端子1114、USBインタフェース1112、およびバスBS3を介してエン트리番号を受取り、その受取ったエン트리番号によって指定されるメモリ1415のライセンス領域1415Bに、ステップS566において受理したライセンス(ライセンス鍵Kc、チェックアウト用トランザクションID、コンテンツID、チェックアウト用ACmおよび再生制御情報ACp)を格納する(ステップS551)。

【0363】パーソナルコンピュータ50のライセンス管理モジュール511は、メモリカード110のメモリ1415に格納されたライセンスのエン트리番号と、平文のチェックアウト用トランザクションIDおよびコンテンツIDを含むメモリカード110へ移動しようとする暗号化コンテンツデータ{Dc}Kcと付加情報Dc-infに対するライセンス管理ファイルを生成し、メ

モリカード110へ送信する(ステップS552)。

【0364】メモリカード110のコントローラ1420は、再生端末102を介してライセンス管理ファイルを受信し、メモリ1415のデータ領域1415Cに受信したライセンス管理ファイルを記録する(ステップS553)。

【0365】パーソナルコンピュータ50のライセンス管理モジュール511は、チェックアウト可能数を1減算し、チェックアウト用トランザクションIDとチェックアウト先のメモリカードに固有の公開暗号鍵Kpmc4とを追加してチェックアウト情報を更新する(ステップS554)。そして、ライセンス管理モジュール511は、トランザクションID、コンテンツID、ライセンス鍵Kc、アクセス制限情報ACm、再生期限ACp、および更新したアドレス情報(チェックアウト可能数と、チェックアウト用トランザクションIDと、チェックアウト先のメモリカード110に個別の戸別公開暗号鍵Kpmc4を追加したもの)を新たな機密情報nとして平文の機密ファイルを更新する(ステップS555)。チェックアウト先の個別公開鍵Kpmc4は、個別公開鍵はメモリカードの耐タンパモジュール無いに格納され、かつ、認証による暗号を用いたセキュリティの高い通信手段によって入手するメモリカードごとに固有値を持つため、メモリカード特定する識別情報として適している。

【0366】その後、ライセンス管理モジュール511は、平文の機密ファイルをバイディング鍵Kbによって暗号化してHDD530に記録されている暗号化機密ファイル160を更新する(ステップS556)。

【0367】ライセンス管理モジュール511は、メモリカード110へチェックアウトしようとする暗号化コンテンツデータ{Dc}Kcと付加情報Dc-infとをHDD530から取得し、{Dc}Kc//Dc-infをメモリカード110へ送信する(ステップS557)。メモリカード110のコントローラ1420は、再生端末100を介して{Dc}Kc//Dc-infを受信し(ステップS558)、バスBS4を介して受信した{Dc}Kc//Dc-infをメモリ1415のデータ領域1415Cに記録する(ステップS559)。

【0368】そうすると、パーソナルコンピュータ50のライセンス管理モジュール511は、メモリカード110へチェックアウトした楽曲を追記した再生リストファイルを作成し(ステップS560)、再生リストファイルと、再生リストファイルとの書換指示とをメモリカード110へ送信する(ステップS561)。メモリカード110のコントローラ1420は、再生端末100を介して再生リストと書換指示とを受信し(ステップS562)、バスBS4を介してメモリ1415のデータ領域1415Cに記録されている再生リストファイルを

10

20

30

40

50



受信した再生リストファイルに書換え（ステップS563）、チェックアウト動作が終了する（ステップS564）。

【0369】このようにして、再生端末100に装着されたメモリカード110が正規の機器であること、同時に、クラス証明書Cm3とともに暗号化して送信されたクラス公開暗号鍵K P m3が有効であることを確認した上で、クラス証明書Cm3が禁止クラスリスト、すなわち、クラス公開暗号鍵K P m3による暗号化が破られたクラス証明書リストに記載されていないメモリカードへのチェックアウト要求に対してのみコンテンツデータをチェックアウトすることができ、不正なメモリカードへのチェックアウトおよび解読されたクラス鍵を用いたチェックアウトを禁止することができる。また、ライセンス管理モジュールおよびメモリカードでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、暗号化コンテンツデータおよびライセンスのチェックアウト動作におけるセキュリティを向上させることができる。さらに、このチェックアウト動作を用いることによって、配信サーバ10との通信機能を有さない再生端末100のユーザも、パーソナルコンピュータ50がソフトウェアによって受信した暗号化コンテンツデータおよびライセンスをメモリカードに受信することができ、ユーザの利便性は向上する。

【0370】[チェックイン] 図1に示すデータ配信システムにおいて、パーソナルコンピュータ50のライセンス管理モジュール511からメモリカード110へチェックアウトされた暗号化コンテンツデータおよびライセンスをライセンス管理モジュール511へ戻す動作について説明する。なお、この動作を「チェックイン」という。

【0371】図35～図38は、図30～図34を参照して説明したチェックアウト動作によってメモリカード110へ貸出された暗号化コンテンツデータおよびライセンスを返却して貰うチェックイン動作を説明するための第1～第4のフローチャートである。なお、図35における処理以前に、パーソナルコンピュータ50のユーザは、HDD520に記録されているコンテンツリストファイルとメモリカード110のデータ領域1415Bに記録されている再生リストファイルを取得し、両ファイルに従って、チェックインするコンテンツを決定し、HDD530およびメモリカード110のコンテンツファイルおよびライセンス管理ファイルが特定でき、かつ、メモリカード110のライセンス管理ファイルを取得してていることを前提として説明する。

【0372】図35を参照して、パーソナルコンピュータ50のキーボード560からチェックインリクエスト

が入力されると（ステップS600）、ライセンス管理モジュール511は、バインディング鍵取得処理を行う。図35のステップS601から図36のステップ615の一連の処理がバインディング鍵取得処理であり、配信2のフローチャートにおける図20のステップS270から図21のステップS284の一連の処理と同じである。ゆえに、説明を省略する。

【0373】バインディング鍵K bを取得したライセンス管理モジュール511は、バスBS2を介してHDD530から暗号化機密ファイル160を取得し、その取得した暗号化機密ファイル160をバインディング鍵K bによって復号して平文の機密ファイルを取得する（ステップS616）。その後、ライセンス管理モジュール511は、ライセンス管理ファイルに記録された機密情報番号nに対応する機密ファイル内の機密情報n（ライセンス（トランザクションID、コンテンツID、ライセンス鍵K c、アクセス制限情報A C m、再生期限A C p）、およびチェックアウト情報（チェックアウト可能数、チェックアウト用トランザクションID、チェックアウト先のメモリカードの個別公開暗号鍵K P m c x））を取得する（ステップS617）。そして、ライセンス管理モジュール511は、認証データの送信要求をUSBインターフェース550、端子580、およびUSBケーブル70を介して再生端末100へ送信する（ステップS618）。

【0374】そうすると、再生端末100のコントローラ1106は、端子1114、USBインタフェース1112およびバスBS3を介して認証データの送信要求を受信し、バスBS3およびメモリカードインタフェース1200を介して認証データの送信要求をメモリカード110へ送信する。そして、メモリカード110のコントローラ1420は、端子1426、インタフェース1424およびバスBS4を介して認証データの送信要求を受信する（ステップS619）。

【0375】コントローラ1420は、認証データの送信要求を受信すると、認証データ保持部1400から認証データ{K P m3//Cm3} K P a2をバスBS4を介して読出し、その読出した認証データ{K P m3//Cm3} K P a2をバスBS4、インタフェース1424および端子1426を介して再生端末100へ出力する。そして、再生端末100のコントローラ1106は、メモリカードインタフェース1200およびバスBS3を介して認証データ{K P m3//Cm3} K P a2を受取り、バスBS3、USBインタフェース1112、端子1114およびUSBケーブル70を介してパーソナルコンピュータ50へ認証データ{K P m3//Cm3} K P a2を送信する（ステップS620）。

【0376】パーソナルコンピュータ50のライセンス管理モジュール511は、端子580およびUSBインタフェース550を介して認証データ{K P m3//C

10

20

30

40

50

m3} KPa2を受信し(ステップS621)、その受信した認証データ{Kpm3//Cm3} KPa2をレベル2認証鍵KPaによって復号する(ステップS622)。そして、ライセンス管理モジュール511は、復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード110が正規のメモリカードからのクラス公開暗号鍵Kpm3とクラス証明書Cm3とを保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう(ステップS623)。正当な認証データであると判断された場合、ライセンス管理モジュール511は、クラス公開暗号鍵Kpm3およびクラス証明書Cm3を承認し、受理する。そして、次の処理(ステップS624)へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵Kpm3およびクラス証明書Cm3を受理しないで処理を終了する(ステップS653)。認証の結果、正規のメモリカードであることが認識されると、ライセンス管理モジュール511は、ダミートランザクションIDを生成する(ステップS624)。ダミー用トランザクションIDは、必ず、メモリカード110の格納されている全てのトランザクションIDと異なる値をとり、かつ、ローカル使用のトランザクションIDとして生成する。

【0377】図37を参照して、ライセンス管理モジュール511は、チェックイン用のセッションキーKs2bを生成する(ステップS625)。そして、ライセンス管理モジュール511は、生成したセッションキーKs2bをメモリカード110から受信したクラス公開暗号鍵Kpm3によって暗号化し、暗号化データ{Ks2b} Km3を生成し(ステップS626)、暗号化データ{Ks2b} Km3にダミートランザクションIDを追加したダミートランザクションID//{Ks2b} Km3をUSBインタフェース550、端子580、およびUSBケーブル70を介して再生端末100へ送信する(ステップS627)。再生端末100のコントローラ1106は、端子1114、USBインタフェース1112、およびBS3を介してダミートランザクションID//{Ks2b} Km3を受信し、その受信したダミートランザクションID//{Ks2b} Km3をメモリカードインタフェース1200を介してメモリカード110へ送信する。そして、メモリカード110のコントローラ1420は、端子1426、インタフェース1424およびバスBS4を介してダミートランザクションID//{Ks2b} Km3を受信する(ステップS628)。復号処理部1422は、コントローラ1420からバスBS4を介して{Ks2b} Km3を受取り、Km保持部1421からのクラス秘密復号鍵Km3によって{Ks2b} Km3を復号してセッションキーKs2bを受信する(ステップS629)。そして、

セッションキー発生部1418は、セッションキーKs2cを生成し(ステップS630)、コントローラ1420は、バスBS4を介してメモリ1415のCRL領域1415Aから禁止クラスリストの更新日時CRLdateを取得し、その取得した更新日時CRLdateを切換スイッチ1446へ与える(ステップS631)。

【0378】そうすると、暗号化処理部1406は、切換スイッチ1446の端子を順次切換えることによって取得したセッションキーKs2c、個別公開暗号鍵Kpmc4および更新日時CRLdateを、復号処理部1422によって復号され、切換スイッチ1442の端子Paを介して取得したセッションキーKs2bによって暗号化し、暗号化データ{Ks2c//Kpmc4//CRLdate} Ks2bを生成する。コントローラ1420は、暗号化データ{Ks2c//Kpmc4//CRLdate} Ks2bをバスBS4、インタフェース1424および端子1426を介して再生端末100へ出力し、再生端末100のコントローラ1106は、メモリカードインタフェース1200を介して暗号化データ{Ks2c//Kpmc4//CRLdate} Ks2bを受取る。そして、コントローラ1106は、暗号化データ{Ks2c//Kpmc4//CRLdate} Ks2bをUSBインタフェース1112、端子1114、およびUSBケーブル70を介してパーソナルコンピュータ50へ送信する(ステップS632)。

【0379】パーソナルコンピュータ50のライセンス管理モジュール511は、端子580およびUSBインタフェース550を介して暗号化データ{Ks2c//Kpmc4//CRLdate} Ks2bを受信し(ステップS633)、その受信した暗号化データ{Ks2c//Kpmc4//CRLdate} Ks2bをセッションキーKs2bによって復号し、セッションキーKs2c、個別公開暗号鍵Kpmc4および更新日時CRLdateを受信する(ステップS634)。

【0380】そうすると、ライセンス管理モジュール511は、受理した個別公開暗号鍵Kpmc4がステップS617で取得した機密情報nのチェックアウト情報に含まれる否かを、すなわち、チェックアウトしようとするライセンスのチェックアウト用トランザクションIDに対応して格納されている個別公開暗号鍵Kpmcxと一致するか否かを確認する(ステップS635)。

【0381】受理された個別公開暗号鍵Kpmc4は、暗号化コンテンツデータおよびライセンスのチェックアウトの際に、更新されたチェックアウト情報に含まれるものである(図34のステップS551を参照)。したがって、暗号化コンテンツデータ等のチェックアウト先に対応する個別公開暗号鍵Kpmc4をチェックアウト情報に含ませることによってチェックインの際にチェックアウトしたチェックアウト先を容易に特定することが

できる。

【0382】ステップS635において、個別公開暗号鍵K<sub>Pmc4</sub>がチェックアウト情報に含まれていないときチェックイン動作は終了する(ステップS653)。ステップS635において、個別公開暗号鍵K<sub>Pmc4</sub>がチェックアウト情報に含まれていると、ライセンス管理モジュール511は、ダミーライセンス、つまり、ダミーランザクションID、対応するコンテンツ存在しないダミーコンテンツID、再生に関与し得ないダミーライセンス鍵K<sub>c</sub>(ダミーK<sub>c</sub>と表す。)、移動複製フラグが「移動複製禁止」かつ再生回数が「0」を示すダミーアクセス制限情報AC<sub>m</sub>(ダミーAC<sub>m</sub>と表す。)、およびダミー再生期限AC<sub>p</sub>(ダミーAC<sub>p</sub>と表す。)を個別公開暗号鍵K<sub>Pmc4</sub>によって暗号化し、暗号化データ{ダミーランザクションID//ダミーコンテンツID//K<sub>c</sub>//ダミーAC<sub>m</sub>//ダミーAC<sub>p</sub>}K<sub>mc4</sub>を生成する(ステップS636)。

【0383】ライセンス管理モジュール511は、暗号化データ{ダミーランザクションID//ダミーコンテンツID//ダミーK<sub>c</sub>//ダミーAC<sub>m</sub>//ダミーAC<sub>p</sub>}K<sub>mc4</sub>をセッションキーK<sub>s2c</sub>によって暗号化を行い、暗号化データ{{ダミーランザクションID//ダミーコンテンツID//ダミーK<sub>c</sub>//ダミーAC<sub>m</sub>//ダミーAC<sub>p</sub>}K<sub>mc4</sub>}K<sub>s2c</sub>を生成し、その生成した暗号化データ{{ダミーランザクションID//ダミーコンテンツID//K<sub>c</sub>//ダミーAC<sub>m</sub>//ダミーAC<sub>p</sub>}K<sub>mc4</sub>}K<sub>s2c</sub>をUSBインタフェース550、端子580、およびUSBケーブル70を介して再生端末100へ送信する(ステップS637)。

【0384】再生端末100のコントローラ1106は、端子1114、USBインタフェース1112、およびバスBS3を介して暗号化データ{{ダミーランザクションID//ダミーコンテンツID//ダミーK<sub>c</sub>//ダミーAC<sub>m</sub>//ダミーAC<sub>p</sub>}K<sub>mc4</sub>}K<sub>s2c</sub>を受信する。コントローラ1106は、受信した暗号化データ{{ダミーランザクションID//ダミーコンテンツID//ダミーK<sub>c</sub>//ダミーAC<sub>m</sub>//ダミーAC<sub>p</sub>}K<sub>mc4</sub>}K<sub>s2c</sub>をバスBS3およびメモリカードインタフェース1200を介してメモリカード110へ送信する。そして、メモリカード110のコントローラ1420は、端子1426、端子1424、およびバスBS4を介して{{ダミーランザクションID//ダミーコンテンツID//ダミーK<sub>c</sub>//ダミーAC<sub>m</sub>//ダミーAC<sub>p</sub>}K<sub>mc4</sub>}K<sub>s2c</sub>を受信する(ステップS638)。

【0385】図38を参照して、メモリカード110の復号処理部1412は、{{ダミーランザクションID//ダミーコンテンツID//ダミーK<sub>c</sub>//ダミーAC<sub>m</sub>//ダミーAC<sub>p</sub>}K<sub>mc4</sub>}K<sub>s2c</sub>をバスB

S4を介して受取り、セッションキー発生部1418によって発生されたセッションキーK<sub>s2c</sub>によって復号し、{ダミーランザクションID//ダミーコンテンツID//ダミーK<sub>c</sub>//ダミーAC<sub>m</sub>//ダミーAC<sub>p</sub>}K<sub>mc4</sub>を受取り(ステップS639)。そして、復号処理部1404は、暗号化データ{ダミーランザクションID//ダミーコンテンツID//ダミーK<sub>c</sub>//ダミーAC<sub>m</sub>//ダミーAC<sub>p</sub>}K<sub>mc4</sub>を復号処理部1412から受取り、その受取った暗号化データ{ダミーランザクションID//ダミーコンテンツID//ダミーK<sub>c</sub>//ダミーAC<sub>m</sub>//ダミーAC<sub>p</sub>}K<sub>mc4</sub>をK<sub>mc</sub>保持部1402からの個別秘密復号鍵K<sub>mc4</sub>によって復号し、ダミーランザクションID、ダミーコンテンツID、ダミーK<sub>c</sub>、ダミーAC<sub>m</sub>、およびダミーAC<sub>p</sub>を受取り(ステップS640)。

【0386】パーソナルコンピュータ50のライセンス管理モジュール511は、メモリカード110のライセンス管理ファイルに記載されているチェックアウトするライセンスが格納されているエントリ番号を取得して、ダミーライセンスを格納するためのエントリ番号として、USBインタフェース550、端子580、およびUSBケーブル70を介して再生端末102へ送信する(ステップS641)。そうすると、再生端末102のコントローラ1106は、端子1114、USBインタフェース1112、およびバスBS3を介してエントリ番号を受取り、バスBS4を介してその受取ったエントリ番号によって指定されるメモリ1415のライセンス領域1415Bに、ダミーライセンス(ダミーランザクションID、ダミーコンテンツID、ダミーライセンス鍵K<sub>c</sub>、ダミーアクセス制限情報AC<sub>m</sub>、およびダミー再生期限AC<sub>p</sub>)を記録する(ステップS642)。このようにダミーランザクションID、ダミーコンテンツID、ダミーライセンス鍵K<sub>c</sub>、ダミーアクセス制限情報AC<sub>m</sub>、およびダミー再生期限AC<sub>p</sub>を記録することによってメモリカード110へチェックアウトされたライセンスを消去することができる。

【0387】その後、パーソナルコンピュータ50のライセンス管理モジュール511は、チェックアウト情報内のチェックアウト可能数を1だけ増やし、チェックアウト用ランザクションID、およびチェックアウト先のメモリカードの個別公開鍵K<sub>Pmc4</sub>を削除してチェックアウト情報を更新する(ステップS643)。そして、ライセンス管理モジュール511は、ランザクションID、コンテンツID、ライセンス鍵K<sub>c</sub>、アクセス制限情報AC<sub>m</sub>、および再生期限AC<sub>p</sub>と更新したチェックアウト情報とを新たな機密情報nとして平文の機密ファイルを更新する(ステップS644)。その後、ライセンス管理モジュール511は、平文の機密ファイルをバイディング鍵K<sub>b</sub>によって暗号化してHDD5

30に記録されている暗号化機密ファイル160を更新する(ステップS645)。

【0388】そうすると、ライセンス管理モジュール511は、メモリカード100のデータ領域1415Cに記録されているチェックインしたライセンスに対応するコンテンツファイル(暗号化コンテンツデータ{Dc}Kcと付加情報Dc-inf)とライセンス管理ファイルを削除する削除指示をUSBインタフェース550、端子580、およびUSBケーブル70を介して再生端末100へ送信する(ステップS646)。再生端末100のコントローラ1106は、端子1114、USBインタフェース1112、およびバスBS3を介してコンテンツファイル(暗号化コンテンツデータ{Dc}Kcおよび付加情報Dc-inf)とライセンス管理ファイルの削除指示を受信する(ステップS647)。そうすると、コントローラ1106は、(暗号化コンテンツデータ{Dc}Kcおよび付加情報Dc-inf)とライセンス管理ファイルとを削除する指示をメモリカード110へ出力し、メモリカード110のコントローラ1420は、端子1426、インタフェース1424、およびバスBS4を介して暗号化コンテンツデータ{Dc}Kcおよび付加情報Dc-infとライセンス管理ファイルとを削除する指示を受信し、バスBS4を介してメモリ1415の暗号化コンテンツデータ{Dc}Kcおよび付加情報Dc-inf)とライセンス管理ファイルとを削除する(ステップS648)。

【0389】パーソナルコンピュータ50のライセンス管理モジュール511は、チェックインした楽曲を削除した再生リストを作成し(ステップS649)、再生リストと、再生リストの書換指示とをメモリカード110へ送信する(ステップS650)。メモリカード110のコントローラ1420は、再生端末100を介して再生リストと書換指示とを受信し(ステップS651)、バスBS4を介してメモリ1415の再生リストを受信した再生リストに書換え(ステップS652)、チェックイン動作が終了する(ステップS653)。

【0390】このように、暗号化コンテンツデータおよびライセンスをチェックアウトした相手先から暗号化コンテンツデータおよびライセンスを返却して貰うことによって、ライセンスの移動が禁止されてるセキュリティレベルの低いライセンス管理モジュールからおよびライセンスが、セキュリティレベルの高いメモリカードへ貸出され、メモリカードにおいてセキュリティレベルの低いライセンス管理モジュールで取得したライセンスを送信できるため、再生端末においてセキュリティレベルの低いライセンス管理モジュールで取得したライセンスによって再生できる暗号化コンテンツデータを再生して楽しむことができる。

【0391】また、メモリカードへ貸出されたライセンスは、アクセス制限情報ACmによってメモリカードか

ら他の記録機器(メモリカード、ライセンス管理デバイスおよびライセンス管理モジュール)に対して、チェックアウトしたライセンスが出力できないよう指定されているため、貸出したライセンスの流出することはない。貸出したライセンス管理モジュールに対してチェックイン(返却)することで、貸出したライセンスの権利が、貸出したライセンス管理モジュールに戻るようになっている。従って、著作者の意に反して複製ができることを許すものではなく、セキュリティレベルが低下する処理ではなく、著作権も保護されている。

【0392】[再生]次に、図39および図40を参照してメモリカード110に移動、およびチェックアウトされたコンテンツデータの再生端末100(コンテンツ再生デバイスとも言う、以下同じ)における再生動作について説明する。なお、図29における処理以前に、再生端末102のユーザは、再生リストファイルに従って、再生するコンテンツ(楽曲)を決定し、コンテンツファイルを特定し、ライセンス管理ファイルを取得していることを前提として説明する。

【0393】図39を参照して、再生動作の開始とともに、再生端末100のユーザから操作パネル1108を介して再生指示が再生端末100にインプットされる(ステップS1000)。そうすると、コントローラ1106は、バスBS3を介して認証データ保持部1500から認証データ{Kpp1/Cp1}KPa2を読み出し、メモリカードインタフェース1200を介してメモリカード110へ認証データ{Kpp1/Cp1}KPa2を出力する(ステップS1002)。

【0394】そうすると、メモリカード110は、認証データ{Kpp1/Cp1}KPa2を受信する(ステップS1004)。そして、メモリカード110の復号処理部1408は、受信した認証データ{Kpp1/Cp1}KPa2を、KPa保持部1414に保持されたレベル2認証鍵KPa2によって復号し(ステップS1006)、コントローラ1420は復号処理部1408における復号処理結果から、認証処理を行なう。すなわち、認証データ{Kpp1/Cp1}KPa2が正規の認証データであるか否かを判断する認証処理を行なう(ステップS1008)。復号できなかった場合、ステップS1048へ移行し、再生動作は終了する。認証データが復号できた場合、コントローラ1420は、取得したクラス証明書Cp1がメモリ1415のCRL領域1415Aから読み出した禁止クラスリストCRLに含まれるか否かを判断する(ステップS1010)。この場合、クラス証明書Cp1には識別番号が付与されており、コントローラ1420は、受信したクラス証明書Cp1の識別番号が禁止クラスリストCRLの中に存在するか否かを判別する。クラス証明書Cp1が禁止クラスリストデータに含まれると判断されると、ステップS1048へ移行し、再生動作は終了する。

10

20

30

40

50

【0395】ステップS1010において、クラス証明書Cp1が禁止クラスリストデータCRLに含まれていないと判断されると、メモリカード110のセッションキー発生部1418は、再生セッション用のセッションキーKs2を発生させる(ステップS1012)。そして、暗号処理部1410は、セッションキー発生部1418からのセッションキーKs2を、復号処理部1408で復号されたクラス公開暗号鍵Kp1によって暗号化した{Ks2}Kp1をバスBS3へ出力する(ステップS1014)。そうすると、コントローラ1420は、インタフェース1424および端子1426を介してメモリカードインタフェース1200へ{Ks2}Kp1を出力する(ステップS1016)。再生端末100のコントローラ1106は、メモリカードインタフェース1200を介して{Ks2}Kp1を取得する。そして、Kp1保持部1502は、秘密復号鍵Kp1を復号処理部1504へ出力する。

【0396】復号処理部1504は、Kp1保持部1502から出力された、公開暗号鍵Kp1と対になっている秘密復号鍵Kp1によって{Ks2}Kp1を復号し、セッションキーKs2を暗号処理部1506へ出力する(ステップS1018)。そうすると、セッションキー発生部1508は、再生セッション用のセッションキーKs3を発生させ、セッションキーKs3を暗号処理部1506へ出力する(ステップS1020)。暗号処理部1506は、セッションキー発生部1508からのセッションキーKs3を復号処理部1504からのセッションキーKs2によって暗号化して{Ks3}Ks2を出力し、コントローラ1106は、バスBS3およびメモリカードインタフェース1200を介して{Ks3}Ks2をメモリカード110へ出力する(ステップS1022)。

【0397】そうすると、メモリカード110の復号処理部1412は、端子1426、インタフェース1424、およびバスBS4を介して{Ks3}Ks2を入力する(ステップS1024)。

【0398】図40を参照して、復号処理部1412は、セッションキー発生部1418によって発生されたセッションキーKs2によって{Ks3}Ks2を復号して、再生端末100で発生されたセッションキーKs3を受理する(ステップS1026)。

【0399】再生端末のコントローラ1106は、メモリカード110から事前に取得した再生リクエスト曲のライセンス管理ファイルからライセンスの格納されているエントリ番号を取得し、メモリカードインタフェース1200を介してメモリカード110へ取得したエントリ番号を出力する(ステップS1027)。

【0400】エントリ番号の入力に応じて、コントローラ1420は、アクセス制限情報ACmを確認する(ステップS1028)。ステップS1028においては、

メモリのアクセスに対する制限に関する情報であるアクセス制限情報ACmを、具体的には、再生回数を確認することにより、確認することにより、既に再生不可の状態である場合には再生動作を終了し、アクセス制限情報の再生回数に回数制限がある場合にはアクセス制限情報ACmの再生回数を更新(1減ずる)した後に次のステップに進む(ステップS1030)。一方、アクセス制限情報ACmの再生回数によって再生回数が制限されていない場合においては、ステップS1030はスキップされ、アクセス制限情報ACmは更新されることなく処理が次のステップ(ステップS1032)に進行される。

【0401】ステップS1028において、当該再生動作において再生が可能であると判断された場合には、メモリ1415のライセンス領域1415Bに記録された再生リクエスト曲のライセンス鍵Kcおよび再生期限ACpがバスBS4上に出力される(ステップS1032)。

【0402】得られたライセンス鍵Kcと再生期限ACpは、切換スイッチ1446の接点Pfを介して暗号化処理部1406に送られる。暗号化処理部1406は、切換スイッチ1442の接点Pbを介して復号処理部1412より受けたセッションキーKs3によって切換スイッチ1446を介して受けたライセンス鍵Kcと再生期限ACpとを暗号化し、{Kc//ACp}Ks3をバスBS4に出力する(ステップS1034)。

【0403】バスBS4に出力された暗号化データは、インタフェース1424、端子1426、およびメモリカードインタフェース1200を介して再生端末100に送出される。

【0404】再生端末100においては、メモリカードインタフェース1200を介してバスBS3に伝達される暗号化データ{Kc//ACp}Ks3を復号処理部1510によって復号処理を行ない、ライセンス鍵Kcおよび再生期限ACpを受理する(ステップS1036)。復号処理部1510は、ライセンス鍵Kcを復号処理部1516に伝達し、再生期限ACpをバスBS3に出力する。

【0405】コントローラ1106は、バスBS3を介して、再生期限ACpを受理して再生の可否の確認を行なう(ステップS1040)。

【0406】ステップS1040においては、再生期限ACpによって再生不可と判断される場合には、再生動作は終了される。

【0407】ステップS1040において再生可能と判断された場合、コントローラ1106は、メモリカードインタフェース1200を介してメモリカード110のデータ領域1415Cにコンテンツファイルとして記録された暗号化コンテンツデータ{Dc}Kcを要求する。そうすると、メモリカード110のコントローラ1

10

20

30

40

50

420は、メモリ1415から暗号化コンテンツデータ(Dc)Kcを取得し、バスBS4、インタフェース1424、および端子1426を介してメモリカードインタフェース1200へ出力する(ステップS1042)。

【0408】再生端末100のコントローラ1106は、メモリカードインタフェース1200を介して暗号化コンテンツデータ(Dc)Kcを取得し、バスBS3を介して暗号化コンテンツデータ(Dc)Kcを復号処理部1516へ与える。

【0409】そして、復号処理部1516は、暗号化コンテンツデータ(Dc)Kcを復号処理部1510から出力されたコンテンツ鍵Kcによって復号してコンテンツデータDataを取得する(ステップS1044)。

【0410】そして、復号されたコンテンツデータDcは音楽再生部1518へ出力され、音楽再生部1518は、コンテンツデータを再生し、DA変換器1519はデジタル信号をアナログ信号に変換して端子1530へ出力する。そして、音楽データは端子1530から外部出力装置を介してヘッドホン130へ出力されて再生される(ステップS1046)。これによって再生動作が終了する。

【0411】上記においては、メモリカード110に記録された暗号化コンテンツデータを再生端末100によって再生する場合について説明したが、パーソナルコンピュータ50、80に、図7に示すコンテンツ再生デバイス1550を内蔵することによってライセンス管理モジュール511およびライセンス管理デバイス520によって受信された暗号化コンテンツデータを再生することが可能である。なお、ライセンス管理モジュール511によって取得された暗号化コンテンツデータをコンテンツ再生デバイス1550により再生する場合、ライセンス管理モジュール511は、ライセンス管理デバイス520に格納されたバイディング鍵Kbを取得し、HDD530に記録された暗号化機密ファイル160をバイディング鍵Kbによって復号し、平文の機密ファイルからライセンスを読み出してコンテンツ再生デバイス1550へ与える。

【0412】また、パーソナルコンピュータ50、80に暗号化コンテンツデータを再生するソフトウェアに従って機能する再生部を内蔵することによって、ライセンス管理モジュール511が取得した暗号化コンテンツデータをソフトウェアにより再生することが可能である。この場合も、ライセンス管理モジュール511は、ライセンス管理デバイス520に格納されたバイディング鍵Kbを取得し、HDD530に記録された暗号化機密ファイル160をバイディング鍵Kbによって復号し、平文の機密ファイルからライセンスを読み出してコンテンツ再生デバイス1550へ与える。コンテンツ再生デバイス1550を用いたハード的に機密性を持つ再生

(レベル2)に比べて、ソフトウェアによる再生は、ソフト的に機密性を持つ再生(レベル1)であるためセキュリティレベルが低い処理である。ゆえに、ライセンス管理デバイス520にて保持されるライセンスは、このソフトウェアによる再生では使用できない。

【0413】[移動2]図1に示すデータ配信システムにおいて、パーソナルコンピュータ50のライセンス管理モジュール511が取得した暗号化コンテンツデータおよびライセンスをパーソナルコンピュータ80へ移動する動作について説明する。なお、この移動を[移動2]という。

【0414】図41～図48は、ライセンス管理モジュール511が取得した暗号化コンテンツデータおよびライセンスのパーソナルコンピュータ80への移動を説明するための第1～第8のフローチャートである。なお、図41における処理以前に、パーソナルコンピュータ50のユーザは、コンテンツリストファイルに従って、移動するコンテンツを決定し、HDD530およびメモカード110のコンテンツファイルおよびライセンス管理ファイルが特定していることを前提に説明する。また、受信側のパーソナルコンピュータ80におけるライセンス管理モジュールのクラスを識別する自然数wはw=5であり、ライセンス管理モジュールを識別する自然数yはy=5とする。

【0415】図41を参照して、パーソナルコンピュータ50のキーボード560を介してパーソナルコンピュータ50のライセンス管理モジュール511によって取得されたライセンスの移動リクエストが入力されると(ステップS800)、パーソナルコンピュータ50のライセンス管理モジュール511は、バイディング鍵取得処理を行う。図41のステップS801から図42のステップ815の一連の処理がバイディング鍵取得処理であり、配信2のフローチャートにおける図20のステップS270から図21のステップS284の一連の処理と同じである。ゆえに、説明を省略する。

【0416】バイディングライセンスを取得すると、パーソナルコンピュータ50のライセンス管理モジュール511は、バスBS2を介してHDD530から暗号化機密ファイル160を取得し、その取得した暗号化機密ファイル160をバイディング鍵Kbによって復号して平文の機密ファイルを取得する(ステップS816)。その後、パーソナルコンピュータ50のライセンス管理モジュール511は、ライセンス管理ファイルに記録された機密情報番号nに対応する機密ファイル内の機密情報n(トランザクションID、コンテンツID、ライセンス鍵Kc、アクセス制限情報ACm、再生期間ACp、およびチェックアウト情報)を取得する(ステップS817)。

【0417】そうすると、パーソナルコンピュータ50のライセンス管理モジュール511は、取得したアクセ

10

20

30

40

50

ス制限情報ACmに基づいて暗号化コンテンツデータの移動および複製が可能か否かを確認する(ステップS518)、つまり、ライセンス管理モジュール511は、取得したアクセス制限情報ACmの再生回数、移動複製フラグに基づいて、パーソナルコンピュータ80へ移動しようとするライセンスがアクセス制限情報ACmによって暗号化コンテンツデータの移動および複製ができないライセンスになっていないか否かを確認する。

【0418】ステップS818において、暗号化コンテンツデータの移動および複製が禁止されていた場合、ステップS903へ移行し、移動動作は終了する。ステップS818において、暗号化コンテンツデータの移動および複製が禁止されていない場合、ステップS819へ移行する。そして、ライセンス管理モジュール511は、取得したチェックアウト情報に基づいてチェックアウトが可能か否かを確認する(ステップS819)。ステップS819において、チェックアウトが不可能であれば、チェックアウトが禁止されているので、ステップS903へ移行し、チェックアウト動作は終了する。ステップS819において、チェックアウト可能であれば、新たなバイディング鍵を、ライセンス管理デバイス520に格納できるかを確認するためにデバイス確認処理を行なうデバイス確認処理において、ライセンス管理デバイス520が認証できない、あるいは、禁止クラスリストCRLにより、新たなバイディング鍵が記録できない場合には、現状を維持するために、処理は中断する。図42のステップS821から図43のステップ833の一連の処理がデバイス確認処理であり、初期化のフローチャートにおける図10のステップS16から図11のステップS42の一連の処理と同じである。ゆえに、説明を省略する。

【0419】デバイス確認処理が終了すると、パーソナルコンピュータ50のライセンス管理モジュール511は、認証データの送信要求を通信ケーブル90を介してパーソナルコンピュータ80へ送信する(ステップS834)。そうすると、パーソナルコンピュータ80のライセンス管理モジュールは、認証データの送信要求を受信する(ステップS835)。

【0420】パーソナルコンピュータ80のライセンス管理モジュールは、認証データの送信要求を受信すると、認証データ{Kpm5/Cm5}Kpa1をパーソナルコンピュータ50へ送信する(ステップS836)。パーソナルコンピュータ50のライセンス管理モジュール511は、端子580およびUSBインタフェース550を介して認証データ{Kpm5/Cm5}Kpa1を受信し(ステップS837)、その受信した認証データ{Kpm5/Cm5}Kpa1をレベル1認証鍵Kpa1によって復号する(ステップS838)。

【0421】図44を参照して、ライセンス管理モジュ

ール511は、復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード110が正規のメモリカードからのクラス公開暗号鍵Kpm5とクラス証明書Cm5とを保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう(ステップS839)。正当な認証データであると判断された場合、ライセンス管理モジュール511は、公開暗号鍵Kpm3および証明書Cm3を承認し、受理する。そして、次の処理(ステップS840)へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵Kpm5およびクラス証明書Cm5を受理しないで処理を終了する(ステップS903)。認証の結果、正規のメモリカードであることが認識されると、ライセンス管理モジュール511は、次に、メモリカード110のクラス証明書Cm3が禁止クラスリストCRLにリストアップされているかどうかをHDD530に照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここで移動動作を終了する(ステップS903)。一方、メモリカード110のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する(ステップS840)。

【0422】認証の結果、正当な認証データを持つメモリカードを備える再生端末からのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されるとライセンス管理モジュール511は、移動用のセッションキーKs2dを生成する(ステップS841)。そして、ライセンス管理モジュール511は、生成したセッションキーKs2dをパーソナルコンピュータ80から受信したクラス公開暗号鍵Kpm5によって暗号化し、暗号化データ{Ks2d}Km5を生成し(ステップS842)、暗号化データ{Ks2d}Km5にトランザクションIDを追加したトランザクションID/{Ks2d}Km5を通信ケーブル90を介してパーソナルコンピュータ80へ送信する(ステップS843)。パーソナルコンピュータ80のライセンス管理モジュールは、トランザクションID/{Ks2d}Km5を受信する(ステップS844)。そして、パーソナルコンピュータ80のライセンス管理モジュールは、クラス秘密復号鍵Km3によって{Ks2d}Km5を復号してセッションキーKs2dを受理する(ステップS845)。そして、パーソナルコンピュータ80のライセンス管理モジュールは、セッションキーKs2eを生成し(ステップS846)、HDDから禁止クラスリストCRLの更新日時CRLdateを取得する(ステップS847)。

【0423】そして、パーソナルコンピュータ80のライセンス管理モジュールは、セッションキーKs2e、個別公開暗号鍵Kpmc5および禁止クラスリストCRLdateをセッションキーKs2dによって暗号化

10

20

30

40

50

し、暗号化データ {Ks2e//KPmc5//CRLdate} Ks2dを生成し、暗号化データ {Ks2e//KPmc5//CRLdate} Ks2dを通信ケーブル90を介してパーソナルコンピュータ50へ送信する(ステップS848)。

【0424】パーソナルコンピュータ50のライセンス管理モジュール511は、端子580およびUSBインタフェース550を介して暗号化データ {Ks2e//KPmc5//CRLdate} Ks2dを受信し(ステップS849)、その受信した暗号化データ {Ks2e//KPmc5//CRLdate} Ks2dをセッションキーKs2dによって復号し、セッションキーKs2e、個別公開暗号鍵KPmc5および更新日時CRLdateを受信する(ステップS850)。そして、ライセンス管理モジュール511は、トランザクションID、コンテンツID、ライセンス鍵Kc、アクセス制限情報ACm、および再生期限ACpをパーソナルコンピュータ80に固有の個別公開暗号鍵KPmc5によって暗号化して暗号化データ {トランザクションID//コンテンツID//Kc//ACm//ACp} Kmc5を生成する(ステップS851)。

【0425】図45を参照して、パーソナルコンピュータ50のライセンス管理モジュール511は、パーソナルコンピュータ80のライセンス管理モジュールから送信された禁止クラスリストの更新日時CRLdateに基づいてパーソナルコンピュータ80のライセンス管理モジュールが管理する禁止クラスリストと自身の管理する禁止クラスリストのどちらが新しいか判断し、自身の管理する禁止クラスリストCRLが古いと判断されたとき、ステップS853へ移行する。また、逆に、自身の管理する禁止クラスリストCRLの方が新しいと判断されたときはステップS856へ移行する(ステップS852)。

【0426】自身の管理する禁止クラスリストCRLが古いと判断されたとき、ライセンス管理モジュール511は、暗号化データ {トランザクションID//コンテンツID//Kc//ACm//ACp} Kmc5をライセンス管理モジュール511において発生されたセッションキーKs2eによって暗号化を行い、暗号化データ {トランザクションID//コンテンツID//Kc//ACm//ACp} Kmc5} Ks2eを通信ケーブル90を介してパーソナルコンピュータ80へ送信する(ステップS853)。

【0427】そして、パーソナルコンピュータ80のライセンス管理モジュールは、暗号化データ {トランザクションID//コンテンツID//Kc//ACm//ACp} Kmc5} Ks2eを受信し(ステップS854)、暗号化データ {トランザクションID//コンテンツID//Kc//ACm//ACp} Kmc5} Ks2eをセッションキーKs2eによって復号

し、{トランザクションID//コンテンツID//Kc//ACm//ACp} Kmc5を受信する(ステップS855)。その後、ステップS861へ移行する。

【0428】一方、ステップS852において、自身の管理する禁止クラスリストCRLが新しいと判断されると、パーソナルコンピュータ50のライセンス管理モジュール511は、HDD530から禁止クラスリストCRLを取得する(ステップS856)。そして、ライセンス管理モジュール511は、禁止クラスリストCRLと暗号化データ {トランザクションID//コンテンツID//Kc//ACm//ACp} Kmc5とを受けて、セッションキーKs2eによって暗号化して暗号化データ {CRL//トランザクションID//コンテンツID//Kc//ACm//ACp} Kmc5} Ks2eを通信ケーブル90を介してパーソナルコンピュータ80に送信する(ステップS857)。

【0429】パーソナルコンピュータ80は、送信された暗号化データ {CRL//トランザクションID//コンテンツID//Kc//ACm//ACp} Kmc5} Ks2eを受信し(ステップS858)、ライセンス管理モジュールは、セッションキーKs2eを用いて受信データを復号してCRLと暗号化データ {トランザクションID//コンテンツID//Kc//ACm//ACp} Kmc5とを受信する(ステップS859)。

【0430】パーソナルコンピュータ80のライセンス管理モジュールは、HDDに記録された禁止クラスリストCRLを受信したCRLによって書換える(ステップS860)。

【0431】ステップS853、S854、S855は、パーソナルコンピュータ80から送られてきた禁止クラスリストの更新日時CRLdateによってが、受信側のパーソナルコンピュータ80の保持する禁止クラスリストCRLが送信側のパーソナルコンピュータ50の保持する禁止クラスリストCRLの方が新しい場合のライセンス鍵Kc等のパーソナルコンピュータ80への移動動作であり、ステップS854、S855、S856、S857、S860は、受信側のパーソナルコンピュータ80の保持する禁止クラスリストCRLが送信側のパーソナルコンピュータ50の保持する禁止クラスリストCRLの方が古い場合のライセンス鍵Kc等のパーソナルコンピュータ80への移動動作である。

【0432】ステップS855またはステップS860の後、パーソナルコンピュータ80のライセンス管理モジュールは、暗号化データ {トランザクションID//コンテンツID//Kc//ACm//ACp} Kmc5は、個別秘密復号鍵Kmc5によって復号し、ライセンス(ライセンス鍵Kc、トランザクションID、コンテンツID、アクセス制限情報ACmおよび再生期限ACp)を受信する(ステップS861)。そして、ライ



センス管理モジュールは、受理したアクセス制限情報ACmによって再生回数が制限されているか否かを判別し、再生回数が制限されていないときステップS863へ移行し、再生回数が制限されているときステップS864へ移行する(ステップS862)。そして、再生回数が制限されていないとき、ライセンス管理モジュールは、パーソナルコンピュータ50から受信した暗号化コンテンツおよびライセンスを他の装置へ貸出するためのチェックアウト可能数を含むチェックアウト情報を生成する(ステップS863)。この場合、チェックアウトの初期値は「3」に設定される。また、再生回数が制限されているとき、ライセンス管理モジュールは、暗号化コンテンツデータを他の装置へ貸出するためのチェックアウト可能数を「0」に設定してチェックアウト情報を生成する(ステップS864)。その後、図46のステップS880へ移行する。

【0433】ステップS853またはステップS857の後、パーソナルコンピュータ50がライセンスをパーソナルコンピュータ80へ移動すると並行してパーソナルコンピュータ50が保持するバイディングライセンスの書換え動作が行なわれる。ステップS853またはステップS857の後、パーソナルコンピュータ50のライセンス管理モジュール511は、アクセス制限情報ACmに基づいてライセンスの複製が可能か否かを判別する(ステップ865)。そして、ライセンスの複製が可能の場合、図48のステップS898へ以降し、暗号化コンテンツデータ{Dc}Kcと付加情報Dc-infをパーソナルコンピュータ80へ送信する。ステップS865において、ライセンスのアクセス制限情報ACmの移動復号フラグによって移動のみ可の場合、ライセンス管理モジュール511は、HDD530に記録された移動させたライセンスに関するコンテンツリストファイル150のライセンス管理ファイル152nを読み出し、ライセンス管理ファイルに記録された機密情報番号nを、ライセンス無に変更してライセンス管理ファイル152nを更新し(ステップS866)、最初の生成したバイディング鍵Kbと異なる新たにバイディング鍵Kbbを生成する(ステップS867)。そして、ライセンス管理モジュール511は、平文の機密ファイル内の機密情報nを削除し、機密ファイルを新たに生成したバイディング鍵Kbbによって暗号化してHDD530内の暗号化機密ファイル160を更新する(ステップS868)。

【0434】図46を参照して、ライセンス管理モジュール511は、新たに生成したバイディング鍵Kbbをライセンス管理デバイス520に格納するためにステップS869からステップS879のバイディング鍵登録処理を行う。初期化のフローチャートにおける図11のステップS44から図12のステップS66の一連の処理と同じ処理であり、バイディング鍵Kbが、新

たなバイディング鍵Kbbにセッション鍵Ks2bがセッション鍵Ks2cに変更されているのみである。ゆえに、説明を省略する。

【0435】新たなバイディング鍵Kbbの登録が終了すると、図48のステップS898へ移行する。

【0436】図47を参照して、図45のステップS861またはステップS862の後、パーソナルコンピュータ80においては、内蔵するライセンス管理モジュールからのバイディング鍵Kb2の取得、すなわちバイディング鍵の取得処理を行う。パーソナルコンピュータ80においても、パーソナルコンピュータ50と同じであり、ステップS878から図48ステップS893に至る一連の処理がバイディング鍵取得処理であり、配信2のフローチャートにおける図20のステップS270から図21のステップS284に至る一連の処理と同じであり、取得するバイディングライセンス(トランザクションIDb2、コンテンツIDb2、バイディング鍵Kb2、および制御情報ACmb2、ACpb2)に、また、セッション鍵Ks2aとKs2bは、それぞれKs2gとKs2fに変更されているのみである。ゆえに、説明を省略する。

【0437】バイディング鍵Kb2を取得すると、パーソナルコンピュータ80のライセンス管理モジュールは、バスBS2を介してHDD530から暗号化機密ファイル160を取得し、その取得した暗号化機密ファイル160をバイディング鍵Kb2によって復号して平文の機密ファイルを取得する(ステップS895)。その後、ライセンス管理モジュールは、パーソナルコンピュータ50から受信したライセンス(トランザクションID、コンテンツID、ライセンス鍵Kc、アクセス制限情報ACm、再生期限ACp)およびチェックアウト情報を新たな機密情報n2として平文の機密ファイルに追記する(ステップS896)。そして、ライセンス管理モジュールは、平文の機密ファイルをバイディング鍵Kb2によって暗号化してHDDに記録されている暗号化機密ファイル160を更新する(ステップS897)。

【0438】そうすると、パーソナルコンピュータ50のライセンス管理モジュール511は、図45のステップS868およびステップS897が共に終了すると、HDD530に記録されているコンテンツファイル(暗号化コンテンツデータ{Dc}Kcと付加情報Dc-inf)を読み出し、暗号化コンテンツデータ{Dc}Kcと付加情報Dc-infとを通信ケーブル90を介してパーソナルコンピュータ80へ送信する(ステップS898)。

【0439】パーソナルコンピュータ80のライセンス管理モジュールは、暗号化コンテンツデータ{Dc}Kcと付加情報Dc-infとを受信し、暗号化コンテンツデータ{Dc}Kcと付加情報Dc-infとを受理

する(ステップS899)。そして、ライセンス管理モジュールは、受理した暗号化コンテンツデータ{Dc}Kcと付加情報Dc-infとをバスBS2をコンテンツファイルとして介してHDDに記録する(ステップS900)。また、ライセンス管理モジュールは、機密情報番号n2、トランザクションIDおよびコンテンツIDを含む、暗号化コンテンツデータ{Dc}Kcと付加情報Dc-infとを記録したコンテンツファイルに対するライセンス管理ファイルを作成してHDDに記録する(ステップS901)。そして、ライセンス管理モジュールは、HDDに記録されているコンテンツリストファイルのコンテンツファイルに受理したコンテンツの名称を追記し(ステップS902)、移動動作が終了する(ステップS903)。

【0440】このように、パーソナルコンピュータ50のライセンス管理モジュール511が取得した暗号化コンテンツデータのライセンスをバイディング鍵Kbによって管理することによって、パーソナルコンピュータ50からパーソナルコンピュータ80へ暗号化コンテンツデータおよびライセンスを移動することができる。

【0441】実施の形態1によれば、パーソナルコンピュータに内蔵されたライセンス管理モジュールがソフトウェアによって取得した暗号化コンテンツデータのライセンスをライセンス管理デバイスによりハード的に管理されるバイディング鍵によって管理するので、ライセンス管理デバイスによって取得された暗号化コンテンツデータのライセンスと同じように「移動」という概念によって他のパーソナルコンピュータへ暗号化コンテンツデータおよびライセンスを送信することが可能である。

【0442】[実施の形態2]図49を参照して、ライセンス管理モジュール511によって取得された暗号化コンテンツデータのライセンスの実施の形態2における管理方法について説明する。

【0443】コンテンツリストファイル150の構成は実施の形態1における構成と同じである。HDD530には、暗号化機密ファイル160が記録されており、これには、ライセンス管理デバイス520に格納されたトランザクションIDb、コンテンツIDb、およびバイディング鍵Kbと同じものが格納されている。そして、暗号化機密ファイル160は、パーソナルコンピュータ50のCPUのシリアル番号等に依存した、パーソナルコンピュータ50から持ち出し不可能となるように独自の暗号化が施されている。また、ライセンス管理ファイル1522、・・・、152nの内、ライセンス管理モジュール511によって取得されたライセンスに対するライセンス管理ファイルでは、ライセンス管理ファイル1522および152nがそれに当たる。ライセンスおよびチェックアウト情報を含む機密情報を、暗号化機密ファイルと同様に暗号化した暗号化機密情報と、ライセンスに関する平文情報とを含んでいる。バイディン

グライセンスは格納するライセンス管理デバイス520のエントリ番号「0」に常に格納する。

【0444】また、ライセンス管理デバイスにライセンスを格納したライセンスに対するライセンス管理ファイル、ライセンス管理ファイル1521および152nがこれに当たる、暗号化機密情報に換えて、ライセンス管理デバイスのライセンス領域1415Bのライセンスするエントリを特定するエントリ番号化記録されている。他のファイルおよびライセンス領域1415Bの構成については、実施の形態1の図25と同じであるので説明を省略する。

【0445】ライセンス管理ファイル1522、・・・、152nからライセンスを取出すときは、ライセンス管理ファイル1522、・・・、152nが暗号化機密情報含んでいれば、ライセンス管理デバイス520のエントリ番号「0」を送信してライセンス管理デバイス520からバイディング鍵Kbを取得し、その取得したバイディング鍵Kbが暗号化機密ファイル160に格納されたバイディング鍵Kbに一致することを確認する。一致していれば、暗号化機密情報を復号して、ライセンスおよびチェックアウト情報を取得する。一致しなければライセンスの取得は禁止されるので処理を中止する。一方、エントリ番号が含まれる場合には、ライセンス管理デバイス520に処理を任せる。さらには、ライセンス無の場合には、ライセンスは存在しないので処理を中止する。したがって、この実施の形態2においては、セキュリティレベルが低い(レベル1)のライセンスに対する全ての処理において、ライセンス管理デバイス520に格納されたバイディング鍵Kbと暗号化機密ファイル160に格納されたバイディング鍵Kbとが一致しなければライセンス管理ファイル1522、・・・、152nから暗号化コンテンツデータのライセンスを取出すことができないように運用する。

【0446】その結果、この実施の形態2においても、ライセンス管理モジュール511によって取得された暗号化コンテンツデータのライセンスは、バイディング鍵Kbによって管理することができ、実施の形態1で説明したのと同じようにパーソナルコンピュータ50からパーソナルコンピュータ80への暗号化コンテンツデータおよびライセンスの移動が可能となる。

【0447】[初期化]図50～図52は、実施の形態2における暗号化機密ファイル160の初期化を説明するための第1～第3のフローチャートである。図50～図52に示すフローチャートは、図10～図12にフローチャートのステップS66をステップS66aに代えたものであり、それ以外は図10～図12のフローチャートと同じである。したがって、図52を参照して、ステップS64の後、ライセンス管理モジュール511は、トランザクションIDb、コンテンツIDbおよびバイディング鍵Kbを平文の機密ファイルに格納し、

平文の機密ファイルに独自の暗号化を施して暗号化機密ファイル160を作成し、その作成した暗号化機密ファイル160をHDD530に記録する(ステップS66a)。そして、初期化の動作は終了する(ステップS68)。

【0448】[配信2] 図53～図56は、実施の形態2において、ライセンス管理モジュール511から配信サーバ10から暗号化コンテンツデータおよびライセンスを受信するときの動作を説明するための第1～第4のフローチャートである。図53～図56に示すフローチャートは、図17～図21に示すフローチャートのステップS266、S268とステップS288との間のステップをステップS287a～S287aに代えたものであり、その他は、図17～図21に示すフローチャートと同じである。図56を参照して、ステップS266、S268において、チェックアウト情報が生成された後、ライセンス管理モジュール511は、受理したライセンス(トランザクションID、コンテンツID、ライセンス鍵Kc、アクセス制限情報ACmおよび再生期限ACp)とチェックアウト情報とバイディング情報とに独自の暗号化を施して暗号化機密情報を生成する(ステップS286a)。そして、ライセンス管理モジュール511は、生成した暗号化機密情報、トランザクションID、およびコンテンツIDを含むライセンス管理ファイルを作成してHDD530に記録する(ステップS287a)。その後、ステップS288へ移行して上述した各ステップが実行されて暗号化コンテンツデータおよびライセンスの配信動作が終了する。

【0449】[リッピング] 図57および図58は、実施の形態2において、ライセンス管理モジュール511が音楽CDから暗号化コンテンツデータおよびライセンスを取得するリッピングの動作を説明するための第1および第2のフローチャートである。図57および図58に示すフローチャートは、図22～図24に示すフローチャートのステップS708とステップS725との間のステップをステップS720a～ステップS724aに代えたものであり、それ以外は、図22～図24に示すフローチャートと同じである。図58を参照して、ステップS708の後、ライセンス管理モジュール511は、受理したライセンス(トランザクションID、コンテンツID、ライセンス鍵Kc、アクセス制限情報ACmおよび再生期限ACp)とチェックアウト情報とバイディング情報とに独自の暗号化を施して暗号化機密情報を生成する(ステップS723a)。そして、ライセンス管理モジュール511は、生成した暗号化機密情報、トランザクションID、およびコンテンツIDを含むライセンス管理ファイルを作成してHDD530に記録する(ステップS724a)。その後、ステップS725へ移行して上述した各ステップが実行されて暗号化コンテンツデータおよびライセンスのリッピン

グの動作が終了する。

【0450】[チェックアウト] 図59～図63は、実施の形態2において、ライセンス管理モジュール511が取得した暗号化コンテンツデータおよびライセンスを再生端末100に装着されたメモリカード110へチェックアウトする動作を説明するための第1～第5のフローチャートである。図59～図63に示すフローチャートは、図30～図34に示すフローチャートのステップS516、S517をステップS516a、S516b、S517aに代え、ステップS552、S553をステップS552a、S553aに代えたものであり、それ以外は、図30～図34に示すフローチャートと同じである。図60を参照して、ステップS515の後、ライセンス管理モジュール511は、HDD530に記録されている暗号化機密ファイル160を取得し、復号して格納されているバイディング鍵Kbを取得する(ステップS516a)。そして、ライセンス管理モジュール511は、ライセンス管理デバイス520から取得したバイディング鍵Kbが暗号化機密ファイル160から取得したバイディング鍵Kbに一致するか否かを判別し、2つのバイディング鍵Kbが相互に一致しないとき、ステップS564へ移行してチェックアウトの動作は終了する。2つのバイディング鍵Kbが相互に一致するときは、次のステップS517aへ移行する(ステップS516b)。

【0451】ライセンス管理デバイス520から取得したバイディング鍵Kbが暗号化機密ファイル160から取得したバイディング鍵Kbに一致したとき、ライセンス管理ファイルから暗号化機密情報を取得して、復号したライセンス(ライセンス鍵Kc、トランザクションID、コンテンツID、アクセス制限情報ACmおよび再生回数ACp)を得る(ステップS517a)。そして、次のステップS5118へ移行する図63を参照して、ステップS551の後、ライセンス管理モジュール511は、更新したチェックアウト情報を反映させた機密情報に独自の暗号化を施して暗号化機密情報を生成し(ステップS552a)、暗号化機密情報を含むライセンス管理ファイルを更新する(ステップS553a)。その後、ステップS554へ移行して上述した各ステップが実行されて暗号化コンテンツデータおよびライセンスのチェックアウトの動作が終了する。

【0452】このように、ライセンス管理デバイス520に格納されたバイディング鍵が暗号化機密ファイル160に格納されたバイディング鍵に一致する場合だけ、ライセンス管理モジュールは、ライセンス管理ファイルから暗号化コンテンツデータのライセンスを取得する。したがって、実施の形態2においても、バイディング鍵によって暗号化コンテンツデータのライセンスを実質的に管理する。

【0453】[チェックイン] 図64～図67は、実施

の形態2において、ライセンス管理モジュール511が再生端末100に装着されたメモリカード110へチェックアウトした暗号化コンテンツデータおよびライセンスをチェックインする動作を説明するための第1～第4のフローチャートである。図64～図67に示すフローチャートは、図35～図38に示すフローチャートのステップS616、S617をステップS616a、616b、617aに代え、ステップS643、S644をステップS643a、644aに代えたものであり、それ以外は、図35～図38に示すフローチャートと同じである。

【0454】図65を参照して、ステップS615の後、ライセンス管理モジュール511は、HDD530に記録されている暗号化機密ファイル160を取得し、復号して格納されているバインディング鍵Kbを取得する(ステップS616a)。そして、ライセンス管理モジュール511は、ライセンス管理デバイス520から取得したバインディング鍵Kbが暗号化機密ファイル160から取得したバインディング鍵Kbに一致するか否かを判別し、2つのバインディング鍵Kbが相互に一致しないとき、ステップS653へ移行してチェックインの動作は終了する。2つのバインディング鍵Kbが相互に一致するときは、次のステップS618へ移行する(ステップS616b)。

【0455】ライセンス管理デバイス520から取得したバインディング鍵Kbが暗号化機密ファイル160から取得したバインディング鍵Kbに一致したとき、ライセンス管理ファイルから暗号化機密情報を取得して、復号したライセンス(ライセンス鍵Kc、トランザクションID、コンテンツID、アクセス制限情報ACmおよび再生回数ACp)を得る(ステップ617a)。そして、次のステップS5118へ移行する。

【0456】図67を参照して、ステップS642の後、ライセンス管理モジュール511は、更新したチェックアウト情報を反映させた機密情報に独自の暗号化を施して暗号化機密情報を生成し(ステップS644a)、暗号化機密情報を含むライセンス管理ファイルを更新する(ステップS645a)。その後、ステップS646へ移行して上述した各ステップが実行されて暗号化コンテンツデータおよびライセンスのチェックインの動作が終了する。

【0457】[移動2]図68～図74は、実施の形態2において、ライセンス管理モジュール511が受信した暗号化コンテンツデータおよびライセンスをパーソナルコンピュータ50からパーソナルコンピュータ80へ移動する動作を説明するための第1～第7のフローチャートである。図68～図74に示すフローチャートは、図39～図46に示すフローチャートのステップS800とステップS801との間にステップS800a～ステップS800cを挿入し、ステップS815とステッ

プS820との間のステップをステップS816a、817aに代え、ステップS867をステップS867aとステップS867bに代え、ステップS862、S863とステップS897との間のステップをステップS895a～896aに代えたものであり、それ以外は、図39～図46に示すフローチャートと同じである。

【0458】図68を参照して、ライセンス管理モジュール511は、ステップS800の後、ライセンス管理モジュール511は、ライセンス管理ファイルの暗号化機密情報を復号して機密情報(トランザクションID、コンテンツID、ライセンス鍵Kc、アクセス制限情報ACm、再生期限ACp、チェックアウト情報を取得する(ステップS800a)。そして、ライセンス管理モジュール511は、ステップS800aにおいて取得したACmに基づいて暗号化コンテンツデータおよびライセンスの移動および複製が可能か否かを判別する。そして、ライセンス管理モジュール511は、暗号化コンテンツデータおよびライセンスの移動および複製が禁止されているとき、ステップS903へ移行して移動動作は終了し、移動および複製が禁止されていないときステップS800cへ移行する(ステップS800b)。

【0459】ライセンス管理モジュール511は、暗号化コンテンツデータおよびライセンスの移動および複製が可能であるとき、チェックアウト情報に基づいてチェックアウト可能か否かを判別し、不可能なときステップS903へ移行して移動動作は終了し、チェックアウト可能なときステップS801へ移行する。

【0460】図69を参照して、ステップS815の後、ライセンス管理モジュール511は、HDD530に記録されている暗号化機密ファイル160を取得し、復号して格納されているバインディング鍵Kbを取得する(ステップS816a)。そして、ライセンス管理モジュール511は、ライセンス管理デバイス520から取得したバインディング鍵Kbが暗号化機密ファイル160から取得したバインディング鍵Kbに一致するか否かを判別し、2つのバインディング鍵Kbが相互に一致しないとき、ステップS903へ移行して移動の動作は終了する。2つのバインディング鍵Kbが相互に一致するときは、次のステップS820へ移行する(ステップS817a)。

【0461】図72を参照して、ステップS867の後、ライセンス管理モジュール511は、平分の機密ファイルに格納されているバインディング鍵Kbをバインディング鍵Kbbに書換へ(ステップS868a)、独自の暗号化を施した暗号化機密ファイルを生成して、HDD530の暗号化機密ファイルと書き換える(ステップS868b)。次いで、図73のステップS869へ移行する。

【0462】図74を参照してステップS862、S863において、チェックアウト情報が生成された後、ラ

イセンス管理モジュール511は、受理したライセンス（トランザクションID、コンテンツID、ライセンス鍵Kc、アクセス制限情報ACmおよび再生期限ACp）とチェックアウト情報とに独自の暗号化を施して暗号化機密情報を生成する（ステップS895a）。そして、ライセンス管理モジュール511は、生成した暗号化機密情報、トランザクションID、およびコンテンツIDを含むライセンス管理ファイルを作成してHDD530に記録する（ステップS896a）。その後、ステップS897へ移行して上述した各ステップが実行されて暗号化コンテンツデータおよびライセンスの配信動作が終了する。

【0463】その他の部分については、実施の形態1と同じである。実施の形態2によれば、パーソナルコンピュータに内蔵されたライセンス管理モジュールがソフトウェアによって取得した暗号化コンテンツデータのライセンスをライセンス管理デバイスによりハード的に管理されるバイディング鍵によって管理するので、ライセンス管理デバイスによって取得された暗号化コンテンツデータのライセンスと同じように「移動」という概念によって他のパーソナルコンピュータへ暗号化コンテンツデータおよびライセンスを送信することが可能である。

【0464】なお、実施に形態1および2において、ライセンス管理デバイス520には、バイディングライセンスと配信によるライセンスが格納できるとしたが、バイディングライセンス専用の管理デバイスであってもかまわない。

【0465】また、バイディングライセンスを指定するためにエントリ番号を指定したが専用のエントリを持ち、高いレベルのライセンスと区別して扱ってもかまわない。

【0466】今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【図面の簡単な説明】

【図1】 本発明の実施の形態1におけるデータ配信システムを概念的に説明する概略図である。

【図2】 図1に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図3】 図1に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図4】 図1に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図5】 図1に示すデータ配信システムにおける配信サーバの構成を示す概略ブロック図である。

【図6】 図1に示すデータ配信システムにおけるパーソナルコンピュータの構成を示す概略ブロック図であ

る。

【図7】 図1に示すデータ配信システムにおける再生端末の構成を示す概略ブロック図である。

【図8】 図1に示すデータ配信システムにおけるメモリカードの構成を示す概略ブロック図である。

【図9】 図6に示すパーソナルコンピュータに内蔵されたライセンス管理デバイスの構成を示す概略ブロック図である。

【図10】 図1に示すパーソナルコンピュータにおける機密ファイルの初期化を説明するための第1のフローチャートである。

【図11】 図1に示すパーソナルコンピュータにおける機密ファイルの初期化を説明するための第2のフローチャートである。

【図12】 図1に示すパーソナルコンピュータにおける機密ファイルの初期化を説明するための第3のフローチャートである。

【図13】 図1に示すデータ配信システムにおけるセキュリティレベルの高い配信動作を説明するための第1のフローチャートである。

【図14】 図1に示すデータ配信システムにおけるセキュリティレベルの高い配信動作を説明するための第2のフローチャートである。

【図15】 図1に示すデータ配信システムにおけるセキュリティレベルの高い配信動作を説明するための第3のフローチャートである。

【図16】 図1に示すデータ配信システムにおけるセキュリティレベルの高い配信動作を説明するための第4のフローチャートである。

【図17】 図1に示すデータ配信システムにおけるセキュリティレベルの低い配信動作を説明するための第1のフローチャートである。

【図18】 図1に示すデータ配信システムにおけるセキュリティレベルの低い配信動作を説明するための第2のフローチャートである。

【図19】 図1に示すデータ配信システムにおけるセキュリティレベルの低い配信動作を説明するための第3のフローチャートである。

【図20】 図1に示すデータ配信システムにおけるセキュリティレベルの低い配信動作を説明するための第4のフローチャートである。

【図21】 図1に示すデータ配信システムにおけるセキュリティレベルの低い配信動作を説明するための第5のフローチャートである。

【図22】 図1に示すデータ配信システムにおけるリッピングの動作を説明するための第1のフローチャートである。

【図23】 図1に示すデータ配信システムにおけるリッピングの動作を説明するための第2のフローチャートである。

10

20

30

40

50



セキュリティレベルの低い他の配信動作を説明するための第3のフローチャートである。

【図56】 図1に示すデータ配信システムにおけるセキュリティレベルの低い他の配信動作を説明するための第4のフローチャートである。

【図57】 図1に示すデータ配信システムにおけるリッピングの他の動作を説明するための第1のフローチャートである。

【図58】 図1に示すデータ配信システムにおけるリッピングの他の動作を説明するための第2のフローチャートである。

【図59】 図1に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックアウトの他の動作を説明するための第1のフローチャートである。

【図60】 図1に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックアウトの他の動作を説明するための第2のフローチャートである。

【図61】 図1に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックアウトの他の動作を説明するための第3のフローチャートである。

【図62】 図1に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックアウトの他の動作を説明するための第4のフローチャートである。

【図63】 図1に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックアウトの他の動作を説明するための第5のフローチャートである。

【図64】 図1に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックインの他の動作を説明するための第1のフローチャートである。

【図65】 図1に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックインの他の動作を説明するための第2のフローチャートである。

【図66】 図1に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックインの他の動作を説明するための第3のフローチャートである。

【図67】 図1に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックインの他の動作を説明するための第4のフローチャートである。

【図68】 図1に示すデータ配信システムにおける暗号化コンテンツデータおよびライセンスのパーソナルコンピュータ間での他の移動を説明するための第1のフローチャートである。

【図69】 図1に示すデータ配信システムにおける暗号化コンテンツデータおよびライセンスのパーソナルコンピュータ間での他の移動動作を説明するための第2の

フローチャートである。

【図70】 図1に示すデータ配信システムにおける暗号化コンテンツデータおよびライセンスのパーソナルコンピュータ間での他の移動動作を説明するための第3のフローチャートである。

【図71】 図1に示すデータ配信システムにおける暗号化コンテンツデータおよびライセンスのパーソナルコンピュータ間での他の移動動作を説明するための第4のフローチャートである。

【図72】 図1に示すデータ配信システムにおける暗号化コンテンツデータおよびライセンスのパーソナルコンピュータ間での他の移動動作を説明するための第5のフローチャートである。

【図73】 図1に示すデータ配信システムにおける暗号化コンテンツデータおよびライセンスのパーソナルコンピュータ間での他の移動動作を説明するための第6のフローチャートである。

【図74】 図1に示すデータ配信システムにおける暗号化コンテンツデータおよびライセンスのパーソナルコンピュータ間での他の移動動作を説明するための第7のフローチャートである。

【符号の説明】

- 10 配信サーバ、20 配信キャリア、30 インターネット網、40 モデム、50、80 パーソナルコンピュータ、60 CD、70 USBケーブル、90 通信ケーブル、100 再生端末、110 メモリカード、130ヘッドホン、150 コンテンツリストファイル、160 暗号化機密ファイル、302 課金データベース、304 情報データベース、306 CRLデータベース、307 メニューデータベース、308 配信記録データベース、310 データ処理部、312、320、1404、1408、1412、1422、1504、1510、1516、5204、5208、5212、5222 復号処理部、313 認証鍵保持部、315 配信制御部、316、セッションキー発生部、318、326、328、1406、1410、1417、1506、5206、5210、5217、5405 暗号処理部、350 通信装置、510、1106、1420、5220 コントローラ、511 ライセンス管理モジュール、520 ライセンス管理デバイス、530 ハードディスク、540 CD-ROMドライブ、550、1112 USBインタフェース、560 キーボード、570 ディスプレイ、580、1114、1426、1530、5226 端子、1108 操作パネル、1110 表示パネル、1200 メモリカードインタフェース、1400、1500、5200 認証データ保持部、1402、5202 Kmc保持部、1414、5214 KPa保持部、1415、5215 メモリ、1415A、5215A CRL領域、1415B、5215B ライセン

10

20

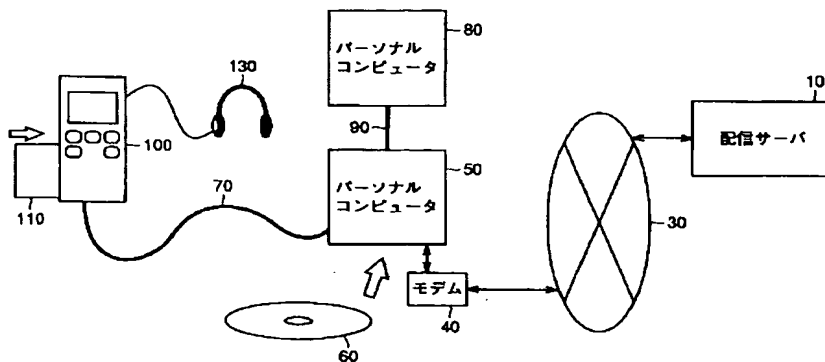
30

40

50

ス領域、1415C データ領域、1416, 5216 \* 切替スイッチ、1502 Kpl保持部、1518 音  
 KPMC保持部、1418, 5218 セッションキ 業再生部、1519 DA交換器、1521~152n  
 ー発生部、1421, 5221 Km保持部、142 ライセンス管理ファイル、1531~153n コン  
 4, 5224 インタフェース、1442, 1446 \* テンツファイル、1550 コンテンツ再生デバイス。

【図1】



【図2】

記号	種類	属性	特性
Dc	コンテンツデータ	コンテンツ固有	例：音楽データ、朗読データ、教材データ、画像データ Kcにて復号可能な暗号化コンテンツデータ (Dc)Kcとして配信され、メモ리카ードに保持される
Dc-Inf	付加情報	コンテンツ固有	Dcに付随する平文データ。
Kc	ライセンス	コンテンツ固有	ライセンス暗号化コンテンツデータを復号する復号鍵
ACm/ACp	ライセンス	ライセンス固有	制限情報 再生やライセンスの取り扱いに対する制限事項
トランザクションID	ライセンス	ライセンス固有	配信を特定するための管理コード
コンテンツID	ライセンス	コンテンツ固有	コンテンツを特定するための管理コード
ライセンスID	ライセンス	ライセンス固有	トランザクションID+コンテンツIDの総称
ライセンス	ライセンス	ライセンス固有	Kc+ACm+ACp+ライセンスIDの総称
CRL	禁止クラスリスト	システム共通	使用禁止認証データのリスト CRLの更新日(CRLdate)を含む

【図4】

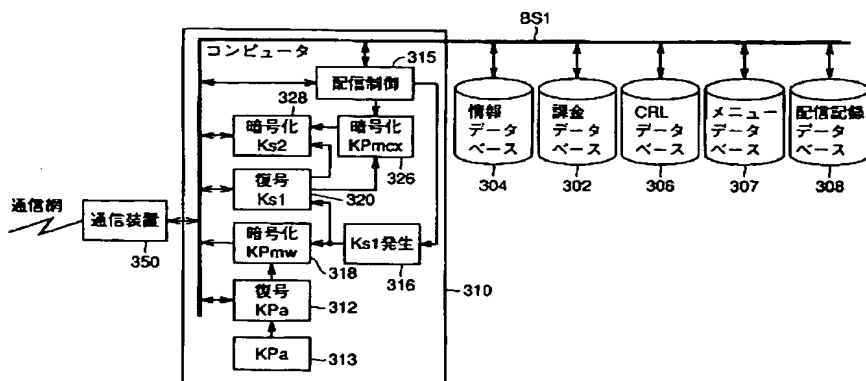
記号	種類	特性
Kb	バイディングライセンス	バイディング鍵 ライセンスおよびチェックアウト管理情報を管理するための共通鍵
ACmb/ACpb		バイディングライセンスに対する制限情報 ACm：固定値(移動・複製禁止/再生回数制限無) ACp：固定値(ダミー/無意味)
トランザクションIDb		バイディングライセンス用のトランザクションID (ライセンスにおけるトランザクションIDとは区別可)
コンテンツIDb		バイディングID用のダミーID
バイディングID		トランザクションIDb+コンテンツIDbの総称
チェックアウト可能数	チェックアウト管理情報	チェックアウト可能なライセンス数 チェックアウトごとに1減算し、チェックインごとに1加算する。
チェックアウト先個別ID		チェックアウト先個別公開暗号鍵KPMcx
チェックアウト時トランザクションID		チェックアウト時に用いられたトランザクションID



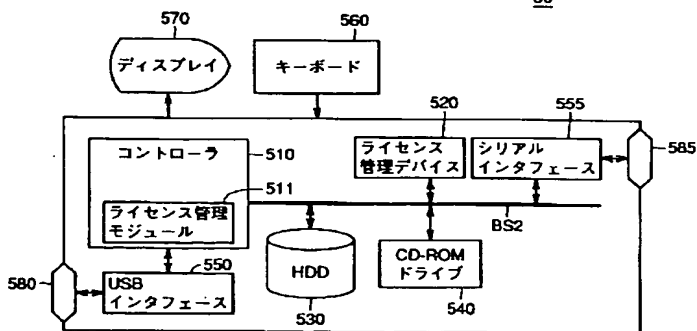
【図3】

	記号	種類	属性	特性
配信サーバ	KPa	公開鍵暗号	システム共有	認証局にて認証された認証データを復号する鍵 セキュリティレベルに応じて2つの認証鍵KPa1(レベル1),KPa2(レベル2)がある。 メモリカードおよびコンテンツ管理モジュールと同一
	Ks1	共通鍵	セッション固有	メモリカード、ライセンス管理デバイス、ライセンス管理モジュールへのライセンス配信ごとに発生 配信サーバと同一
メモリカード	KPa	公開鍵暗号	システム共有	認証局にて認証された認証データを復号する鍵
	KPmw	公開鍵暗号	クラス固有	証明書Cmwとともに認証局にて暗号化された認証データとして保持 wはクラスを識別するための識別子
ライセンス管理デバイス (ハードタンバ)	Kmw	秘密復号鍵	クラス固有	公開鍵暗号KPmwにて暗号化されたデータを復号する非対称な復号鍵
	KPmxc	公開鍵暗号	個別	メモリカードごとに異なる。 xはモジュールを識別するための識別子
ライセンス管理モジュール (ソフトウェア)	Kmxc	秘密復号鍵	個別	公開鍵暗号KPmxcにて暗号化されたデータを復号する非対称な復号鍵
	Ks2	共通鍵	セッション固有	配信サーバまたは音楽再生モジュール間のライセンスの授受ごとに発生
コンテンツ再生デバイス	Cmw	証明書	クラス証明書	メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールのクラス証明書。認証機能を有する。 (KPmw/Cmw)KPaの形式で出荷時に記録。 メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールのクラスwごとに異なる。
	KPpy	公開鍵暗号	クラス固有	証明書Cmwとともに認証局にて暗号化された認証データとして保持 yはクラスを識別するための識別子
コンテンツ再生デバイス	Kpy	秘密復号鍵	クラス固有	公開鍵暗号KPpyにて暗号化されたデータを復号する非対称な復号鍵
	Ks3	共通鍵	セッション固有	配信サーバまたは音楽再生モジュール間の再生セッションごとに発生
	Cpy	証明書	クラス証明書	コンテンツ再生デバイスのクラス証明書。認証機能を有する。 (KPpy/Cpy)KPaの形式で出荷時に記録。 コンテンツ再生デバイスのクラスyごとに異なる。

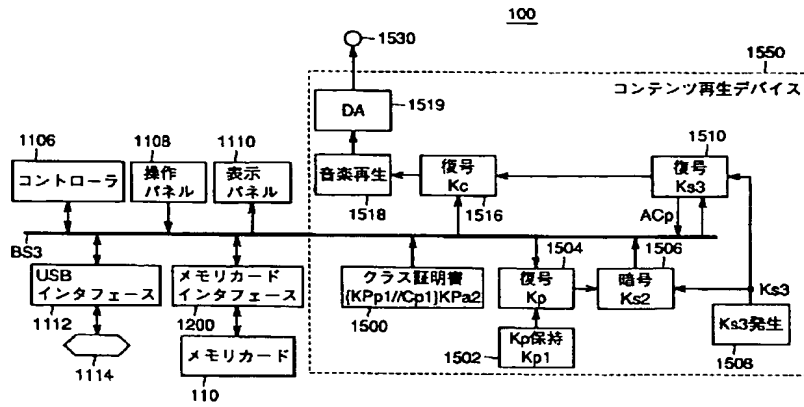
【図5】



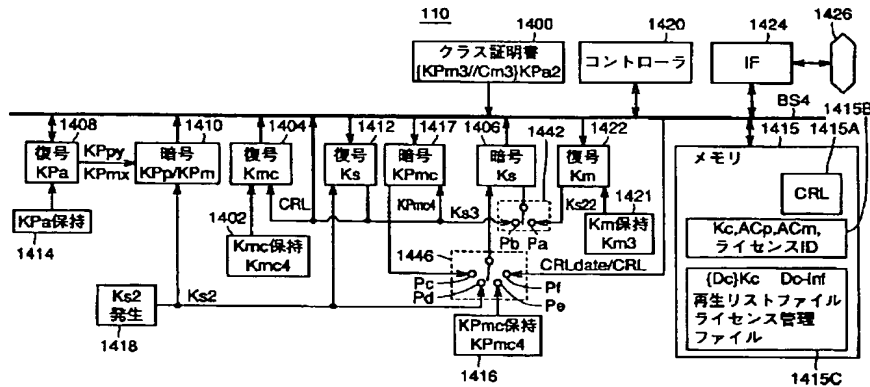
【図6】



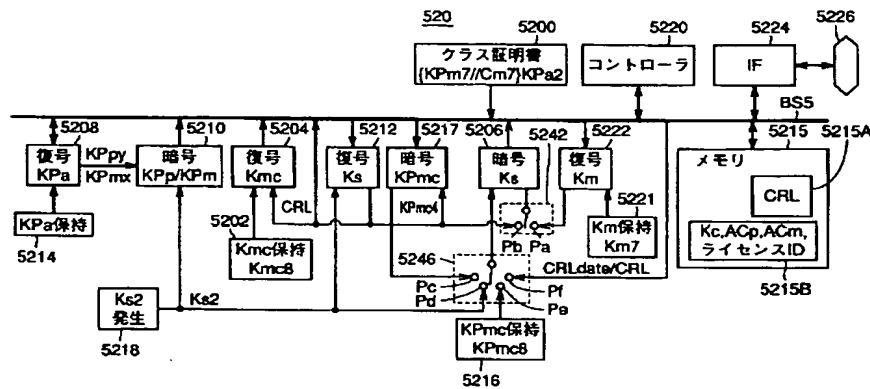
【図7】



【図8】

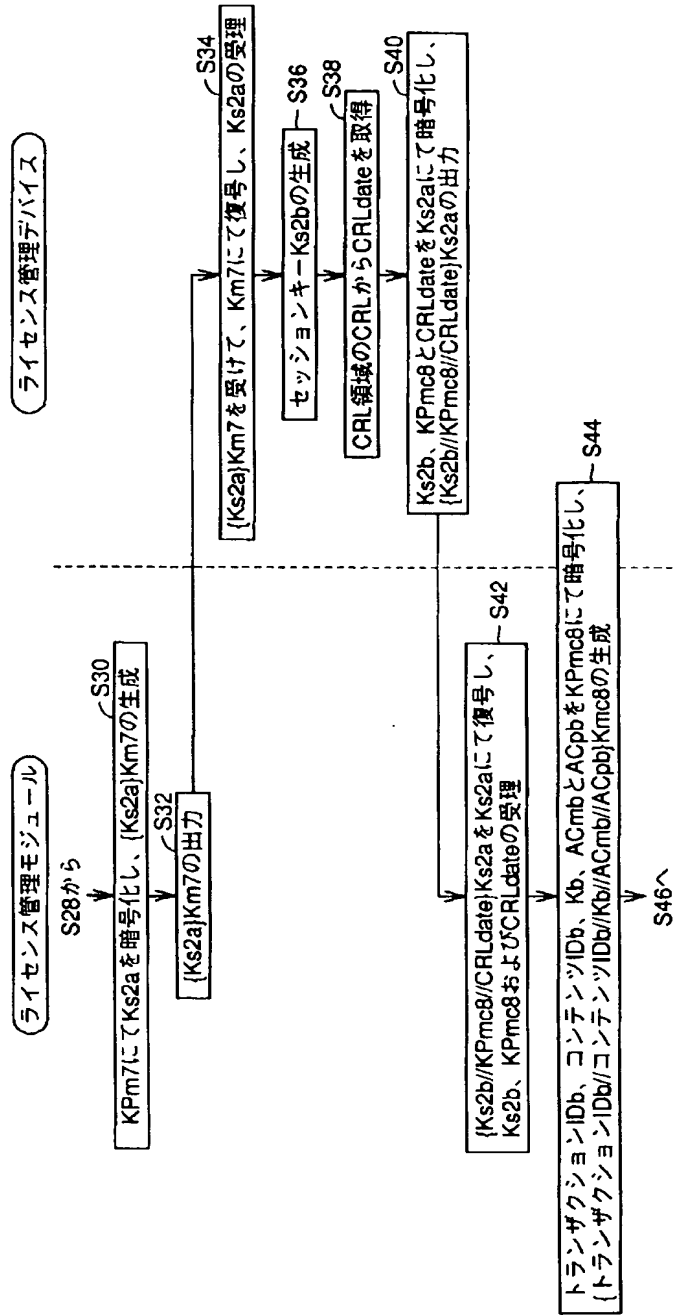


【図9】

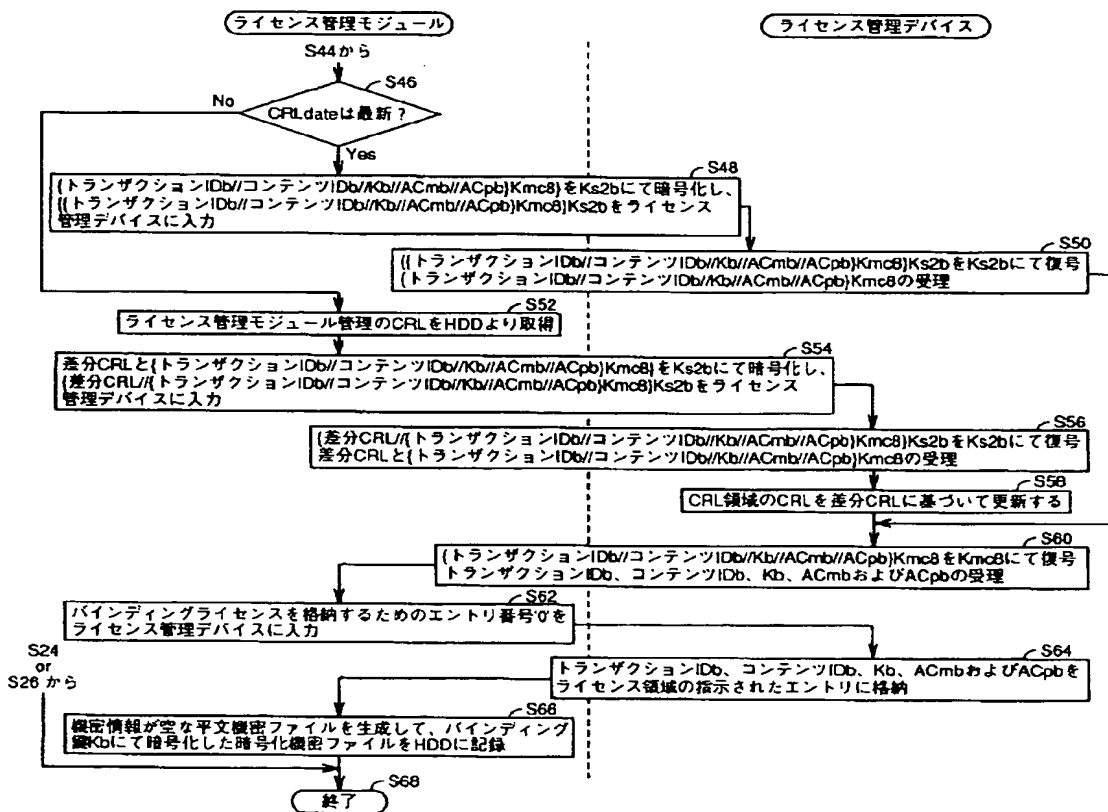




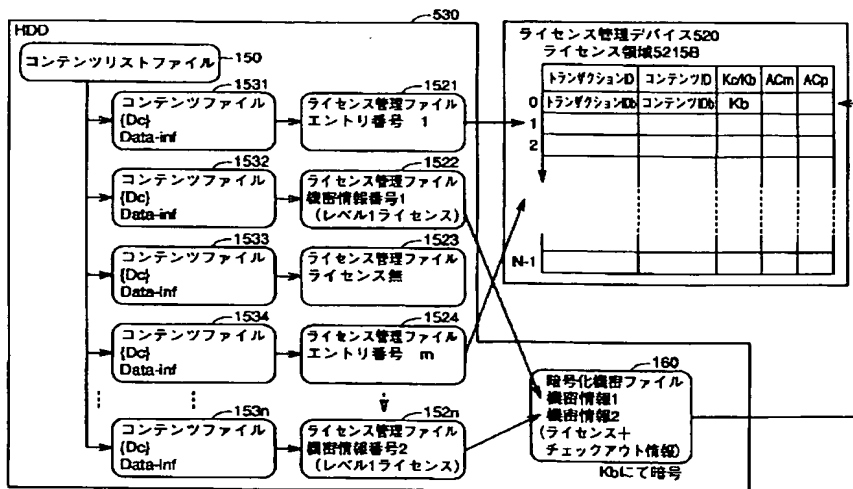
【図11】



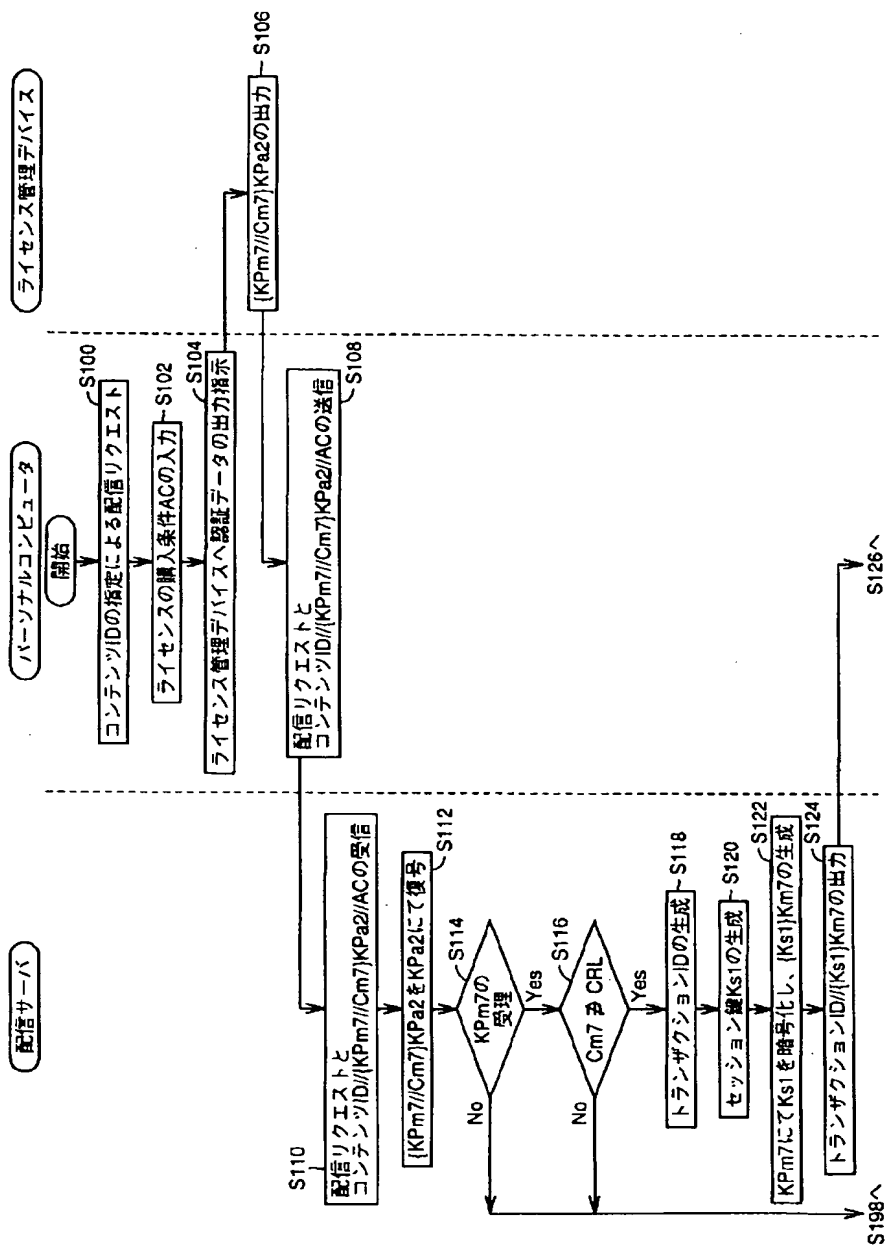
【図12】



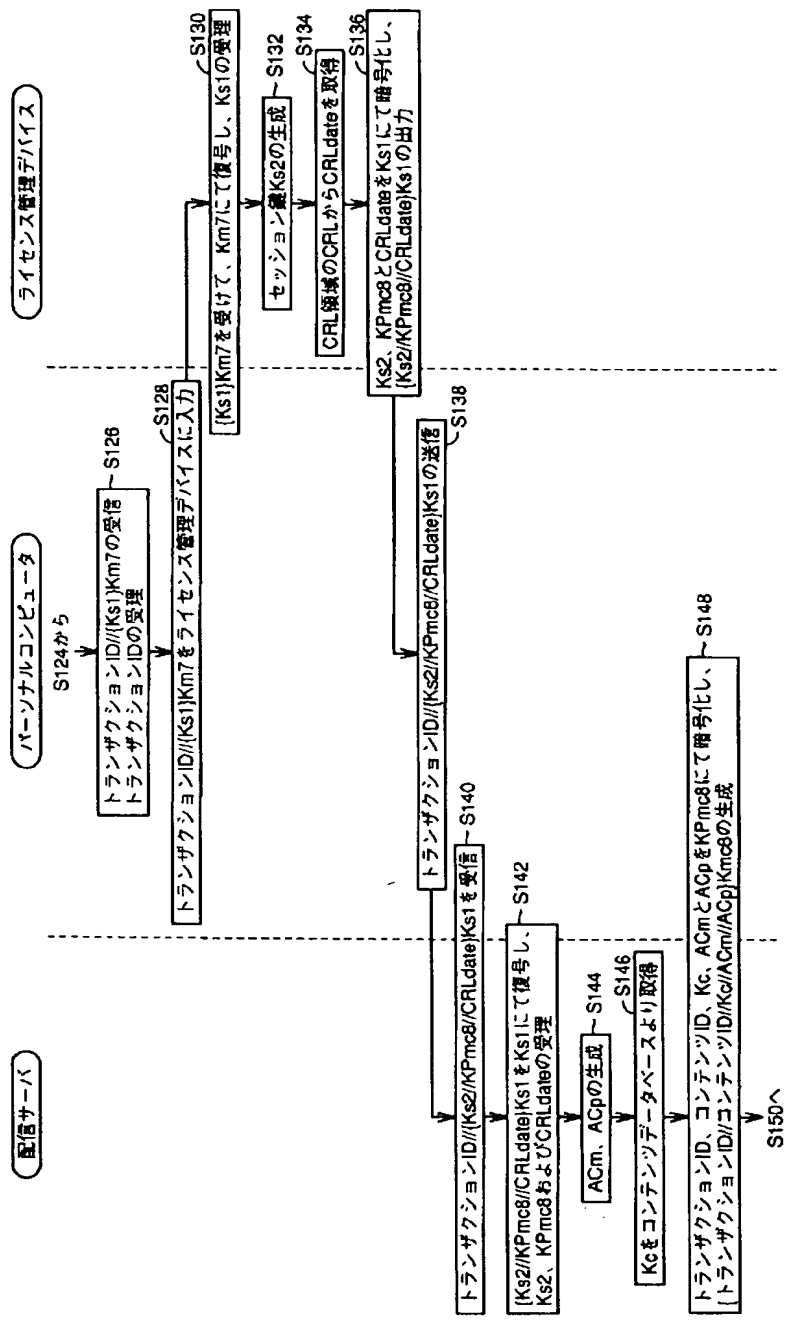
【図25】



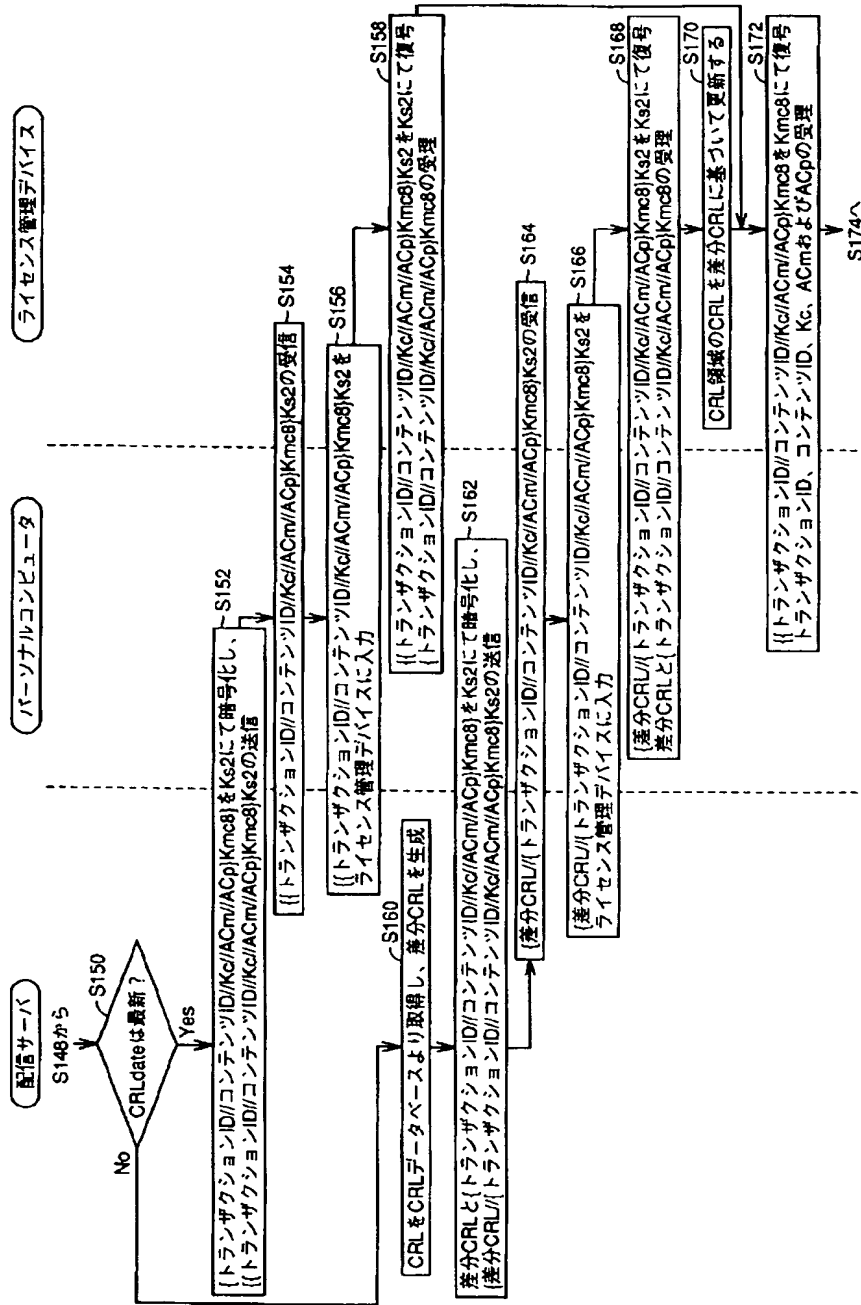
【図13】



【図14】

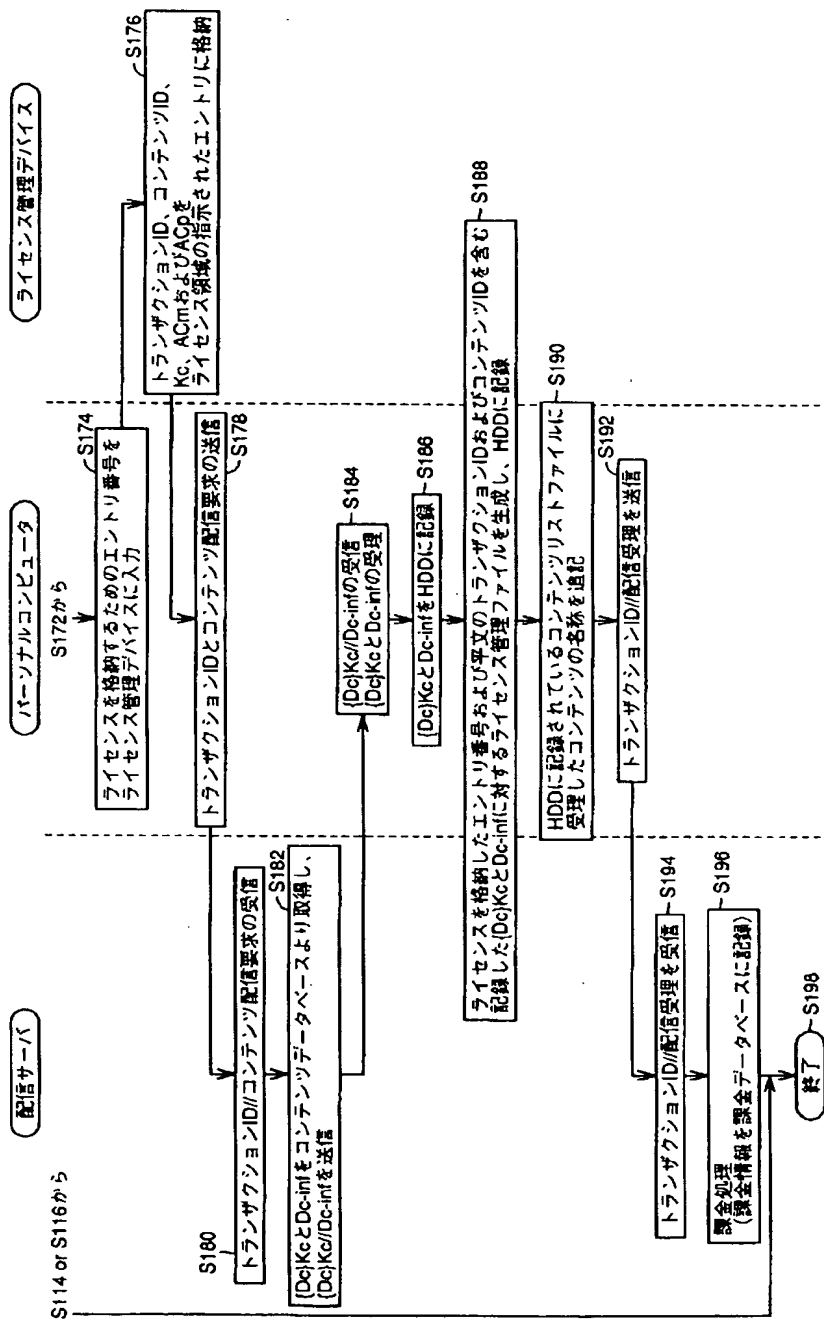


【図15】

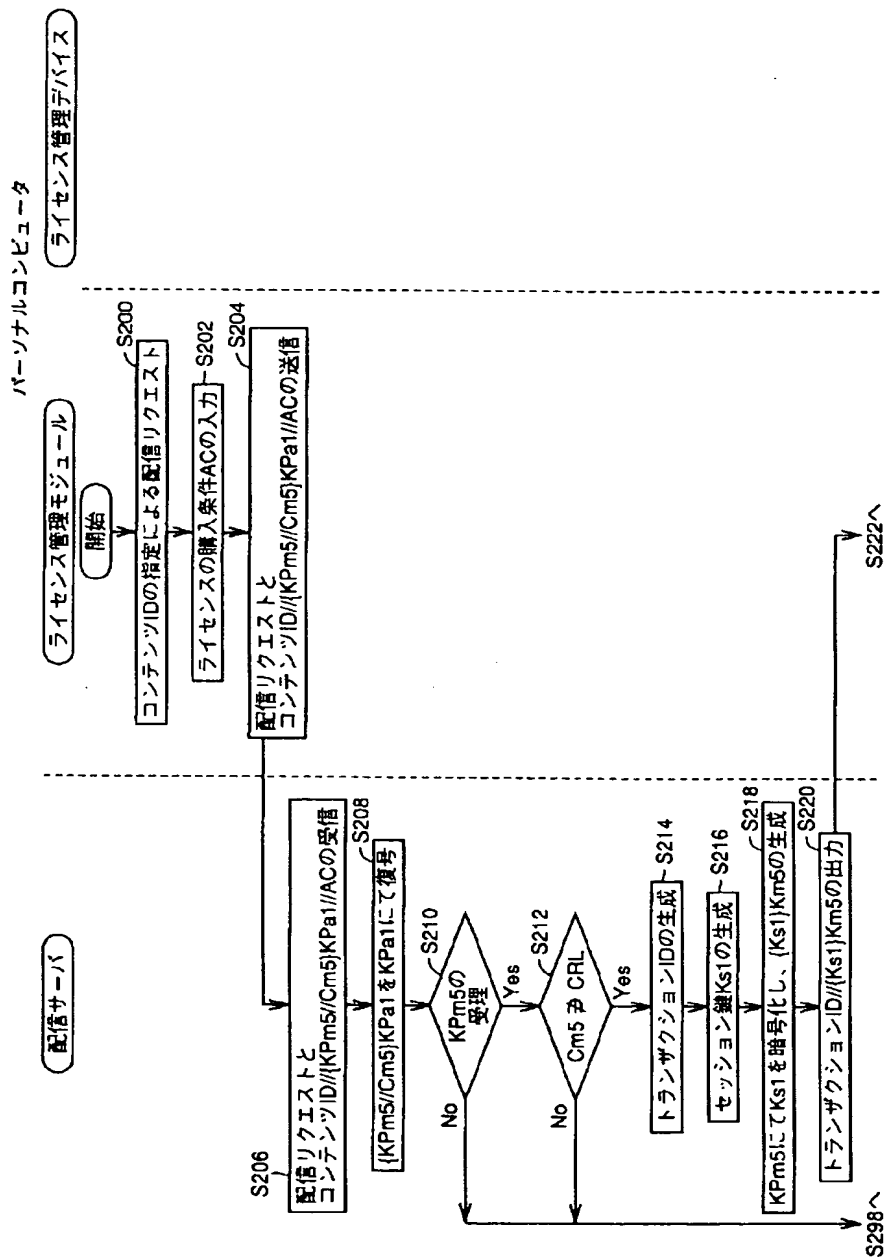




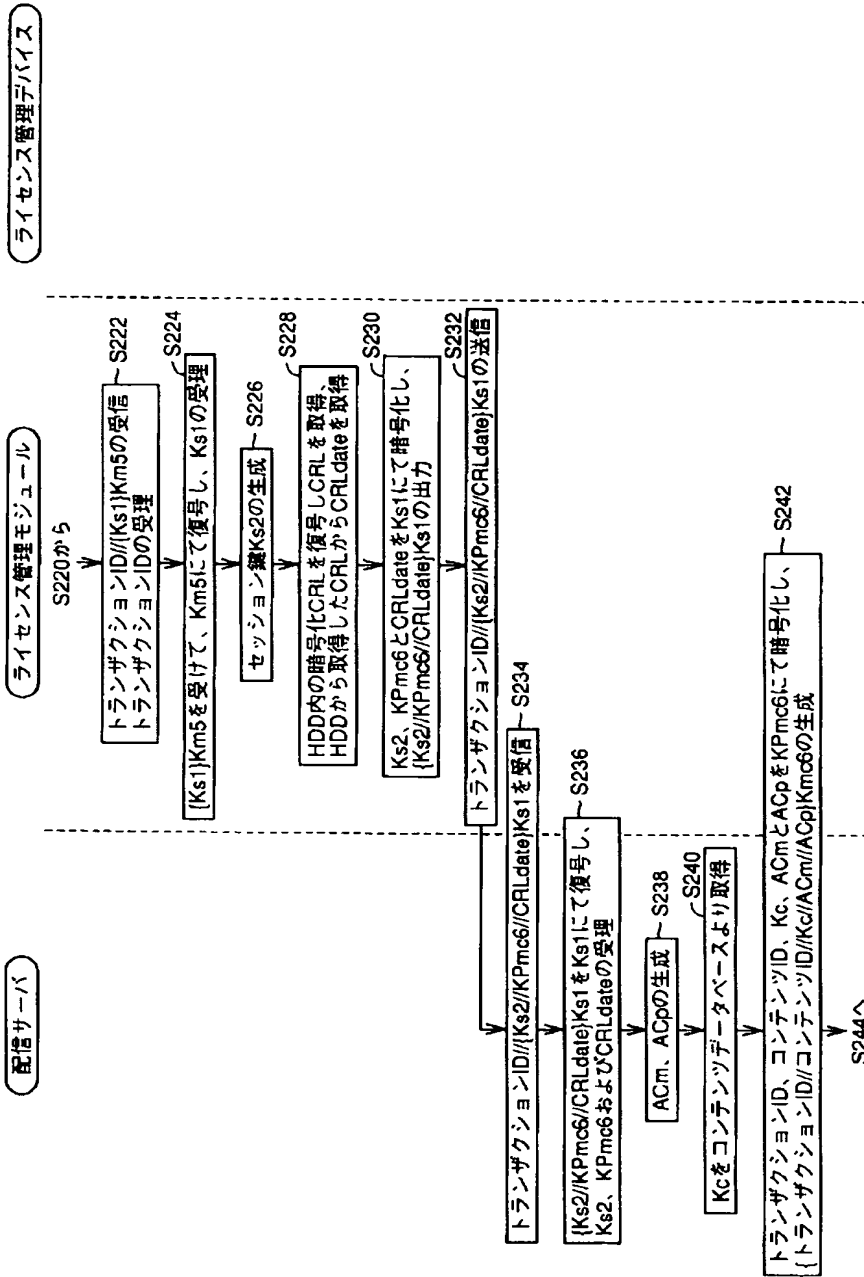
【図16】



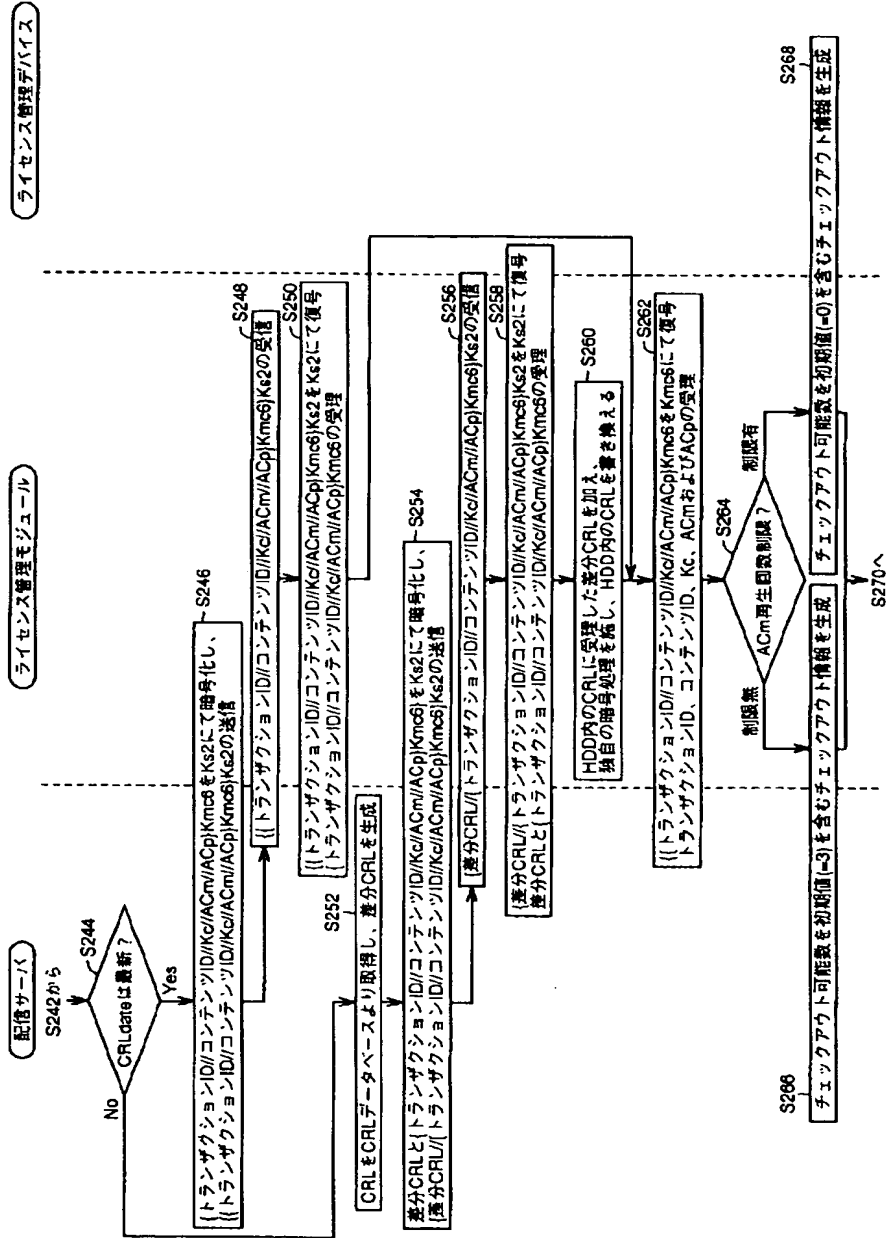
【図17】



【図18】



【図19】

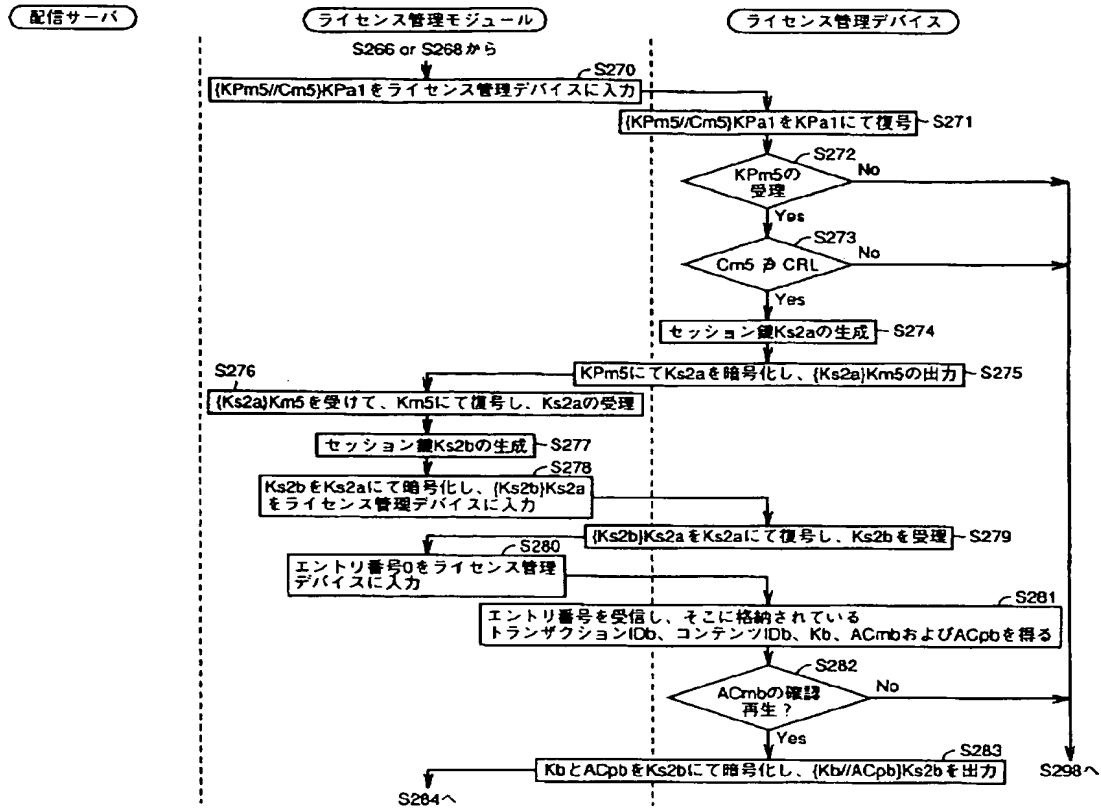


ライセンス管理デバイス

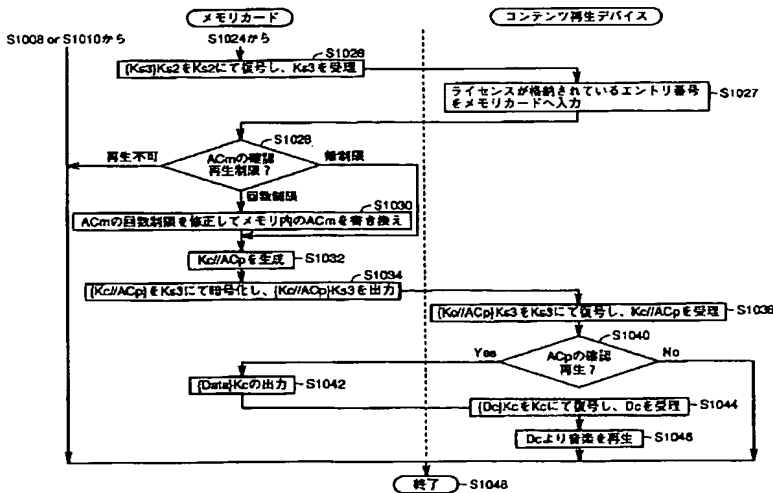
ライセンス管理モジュール

配信サーバ

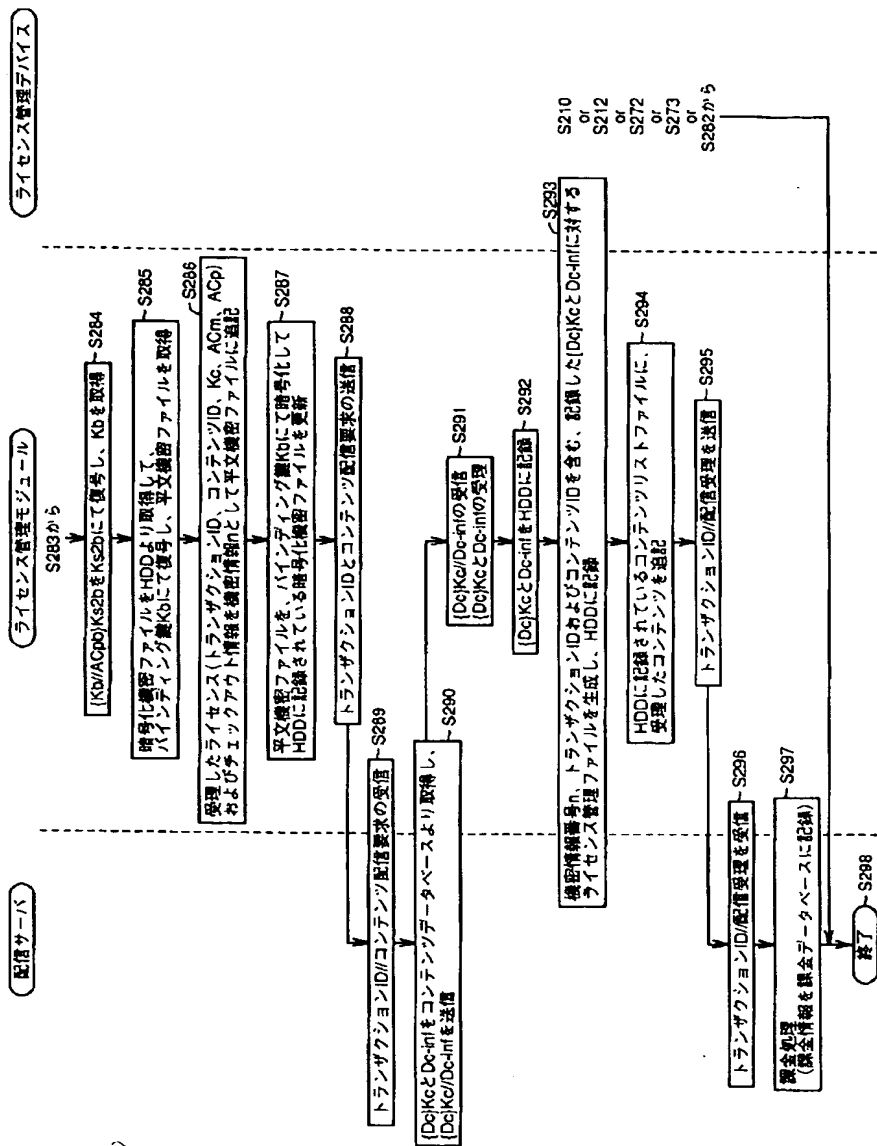
【図20】



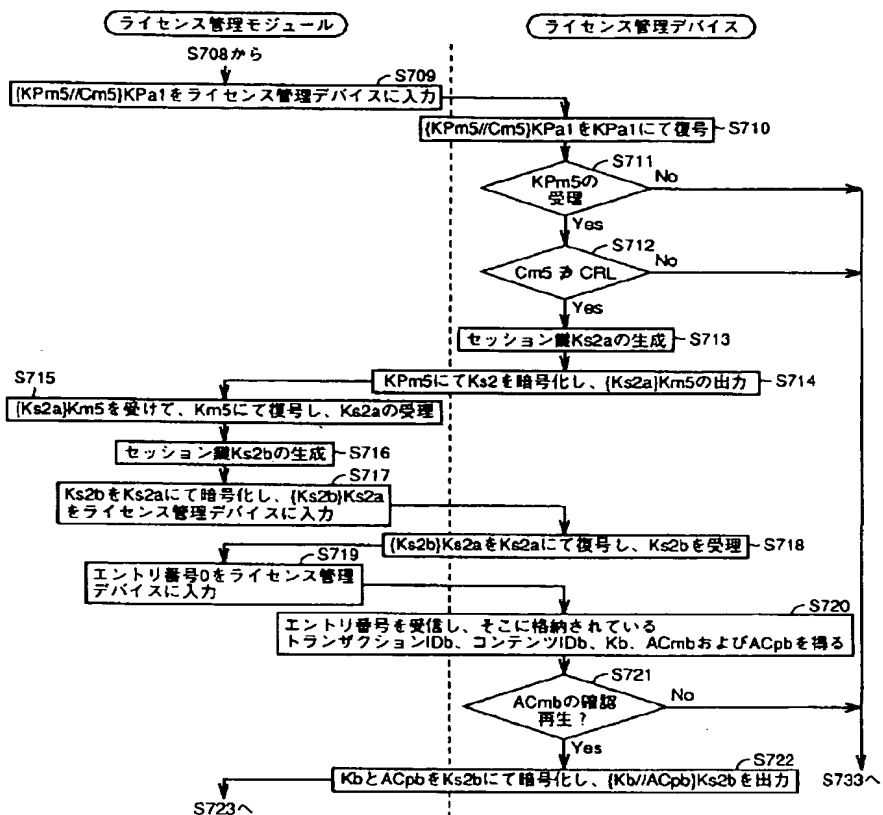
【図40】



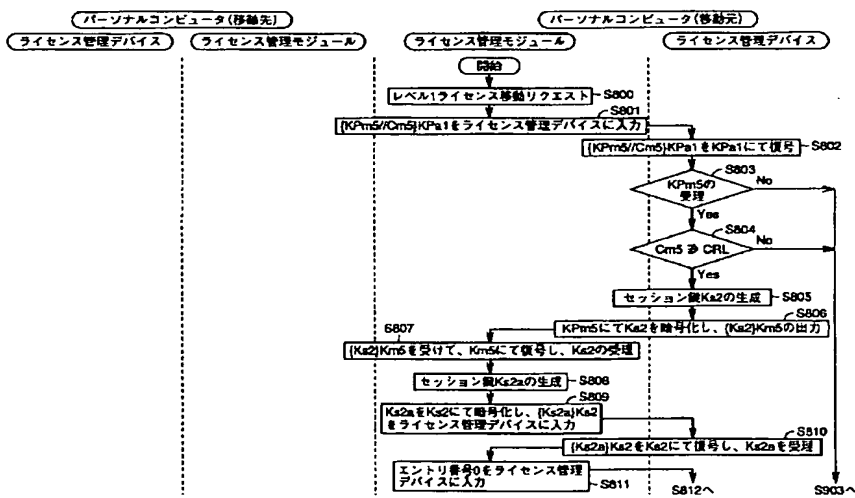
【図21】



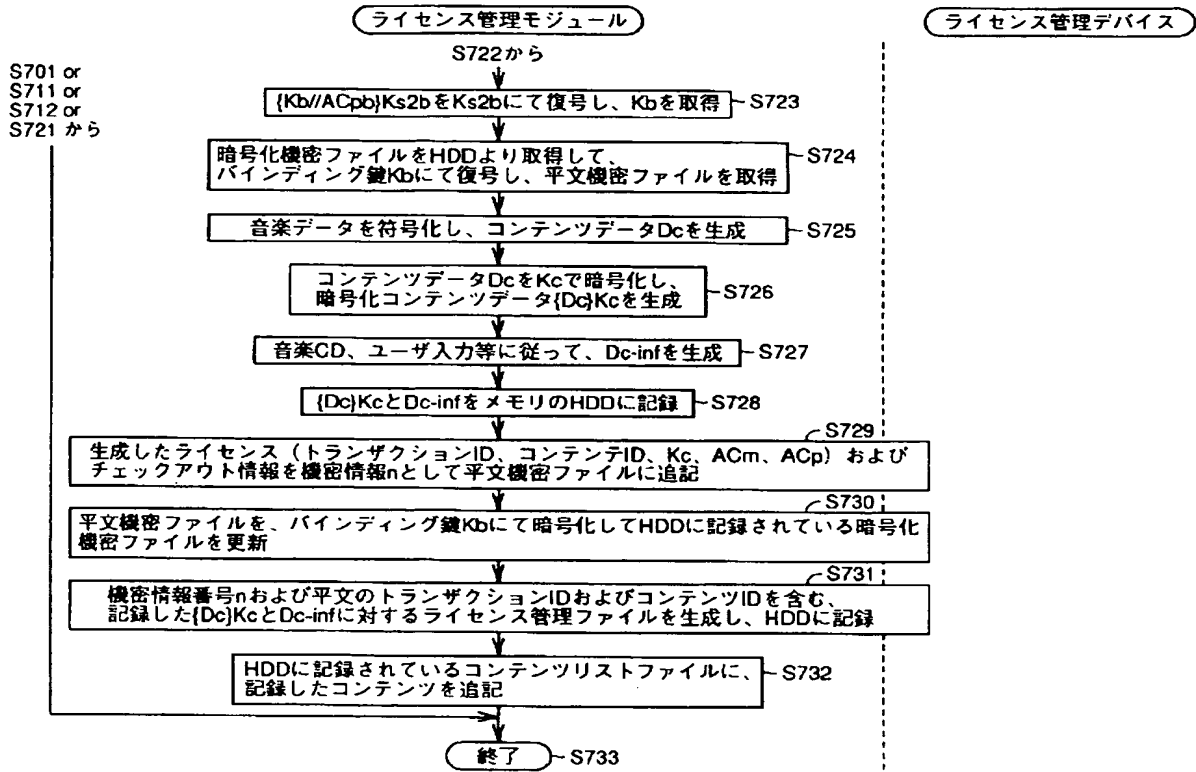
【図23】



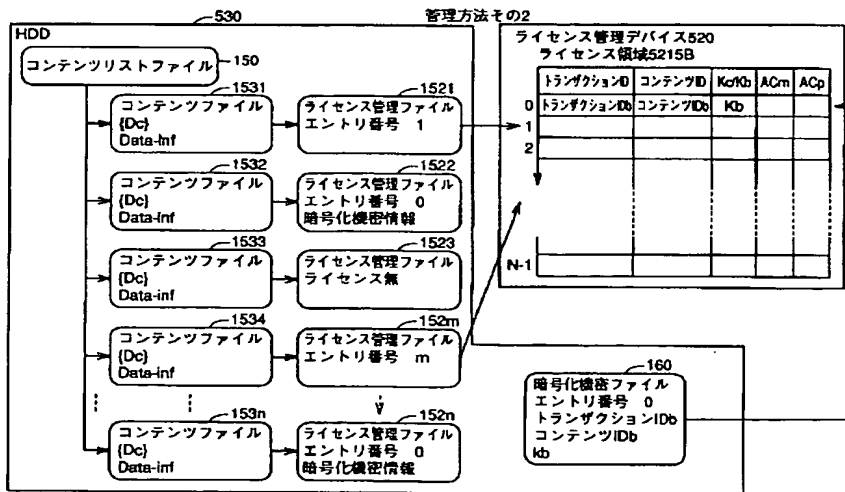
【図41】



【図24】

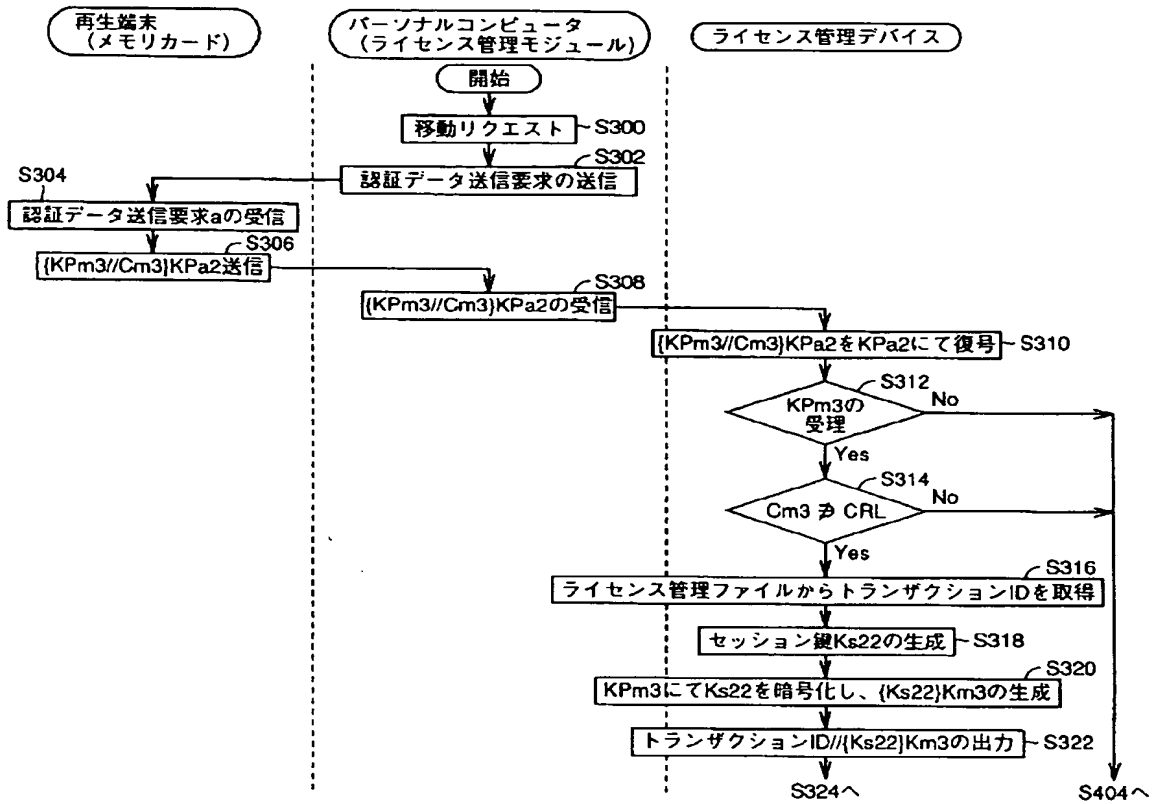


【図49】

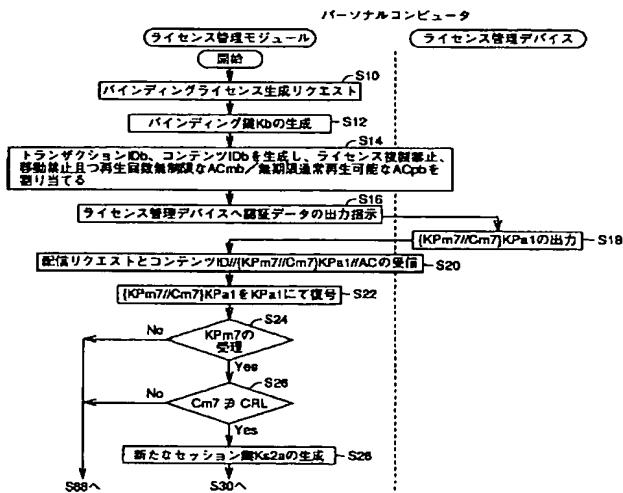




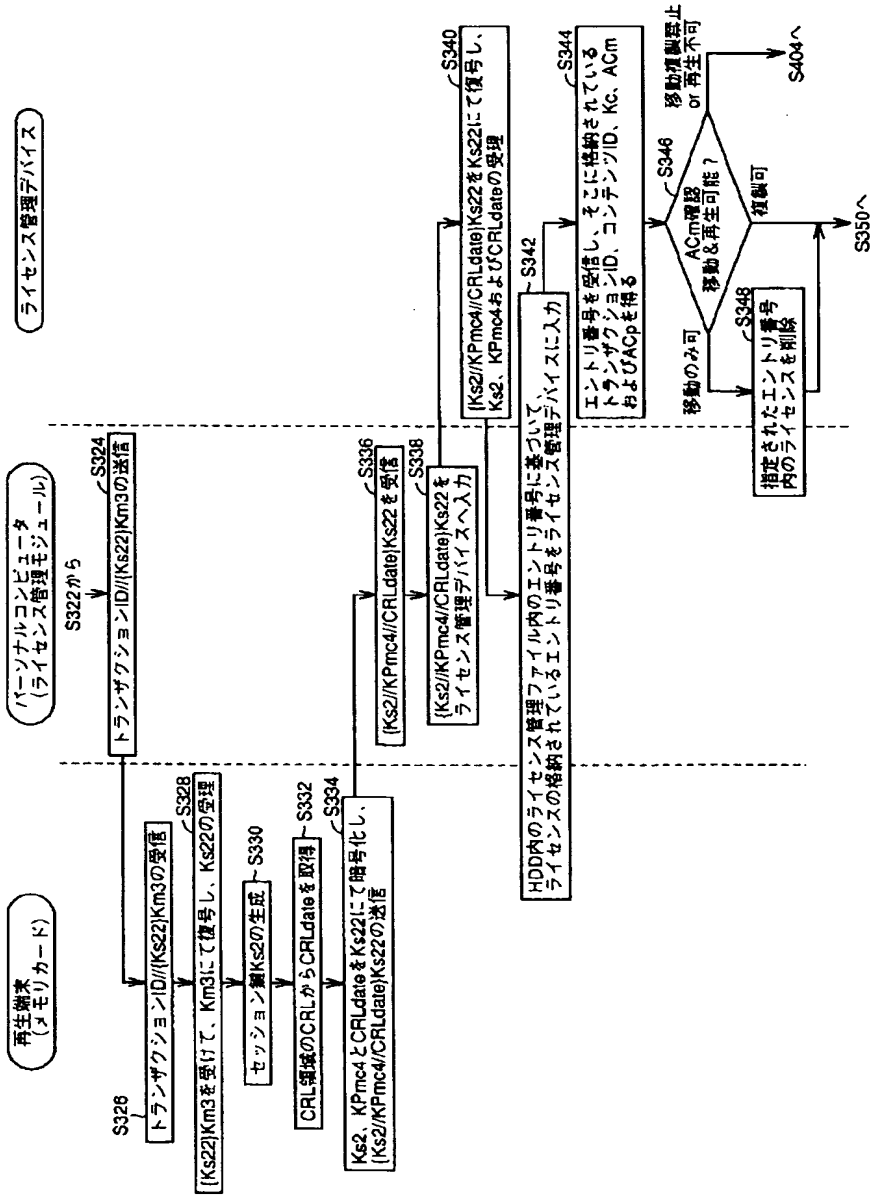
【図26】



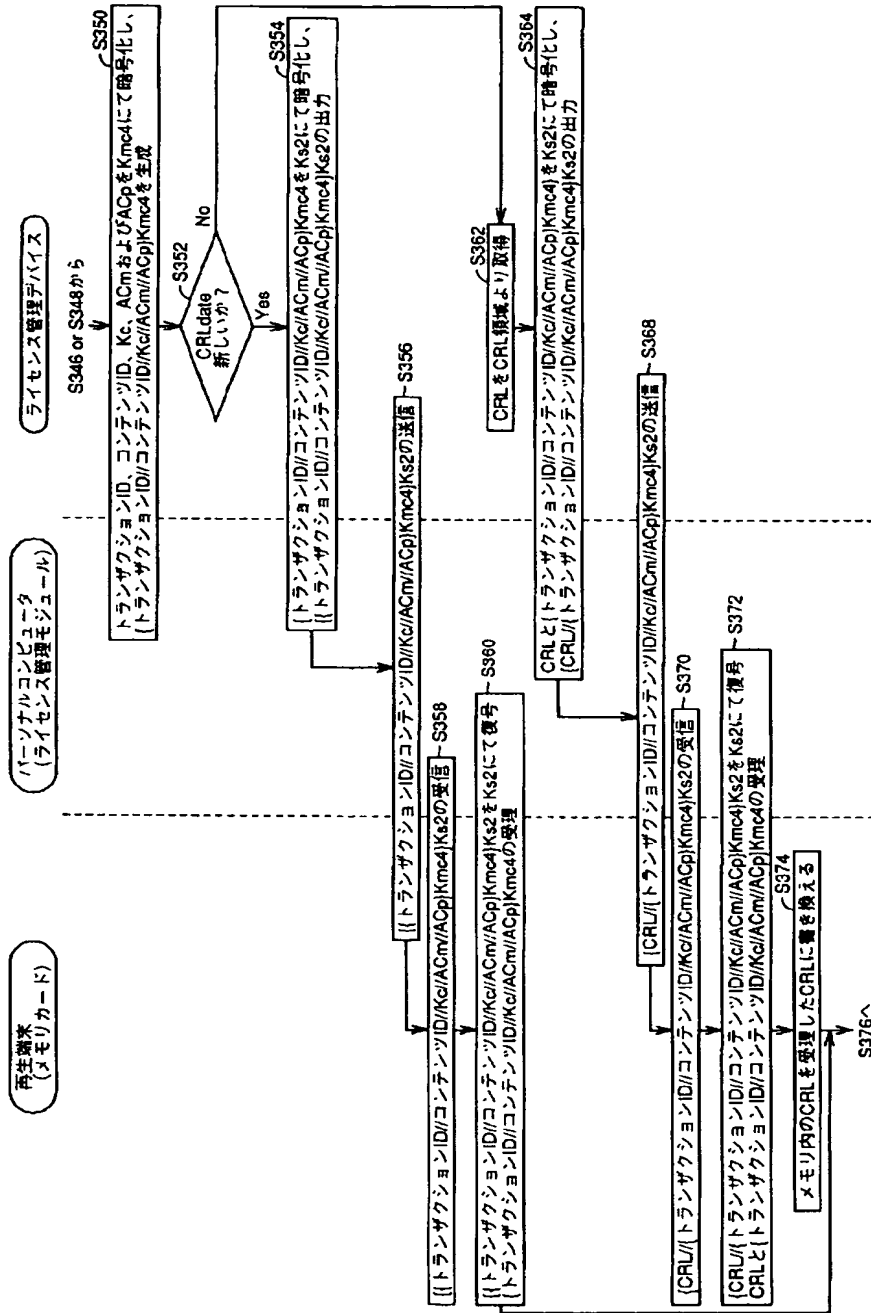
【図50】



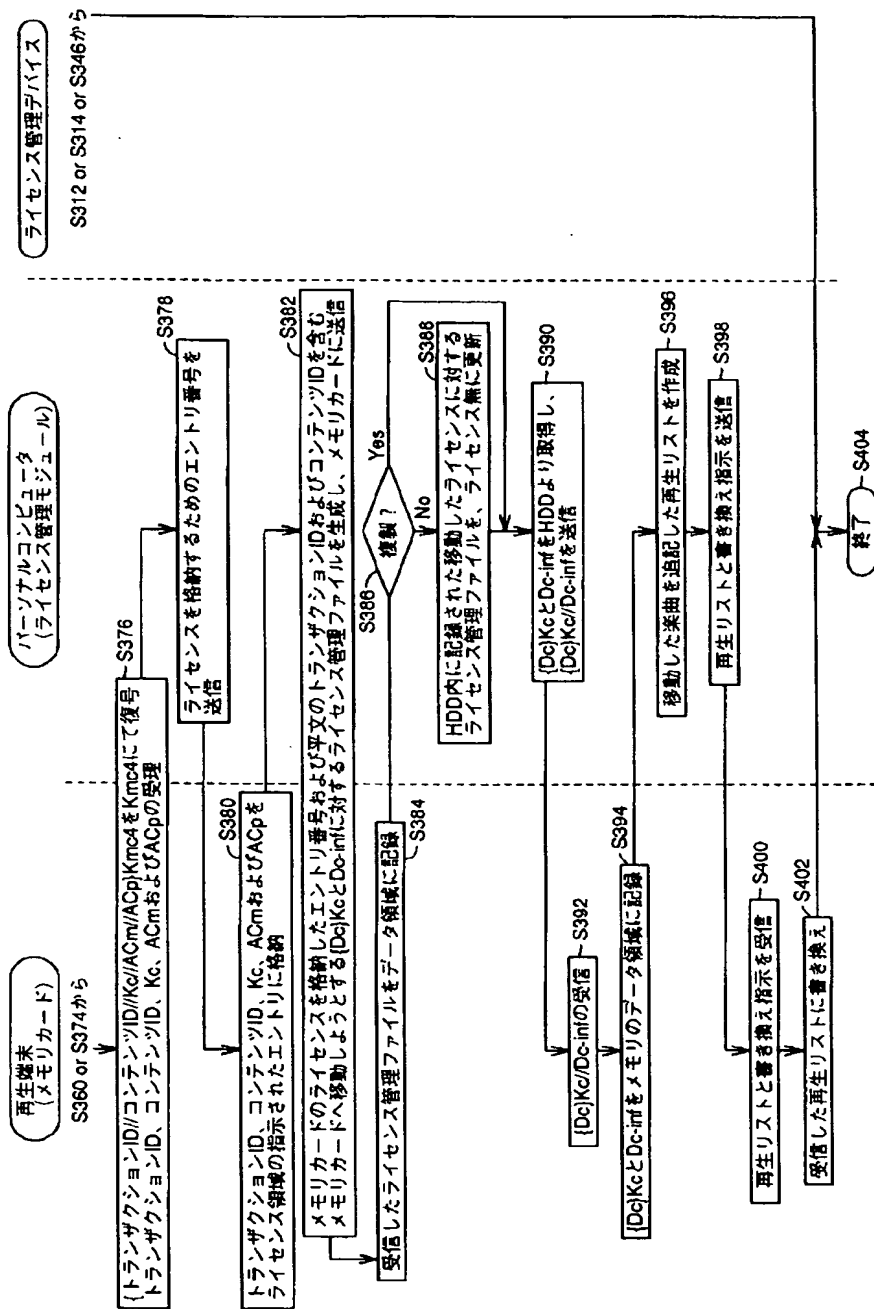
【図27】



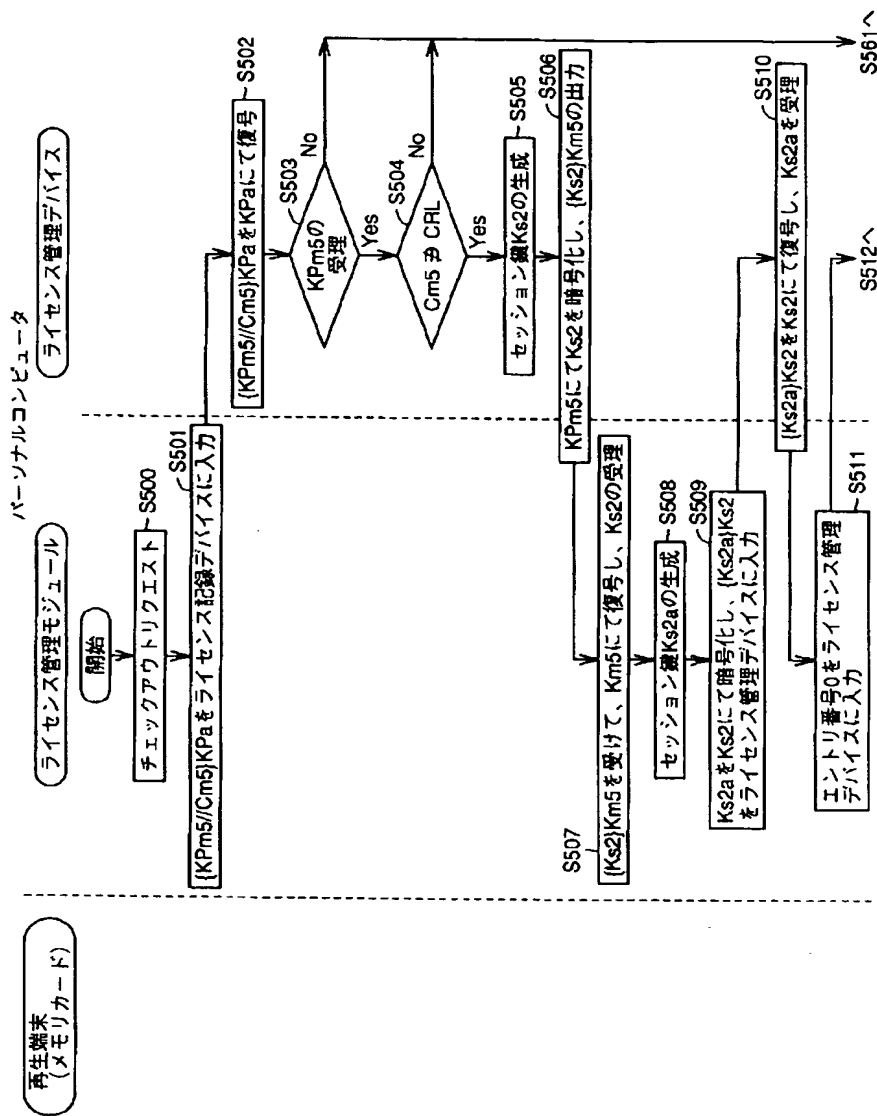
【図28】



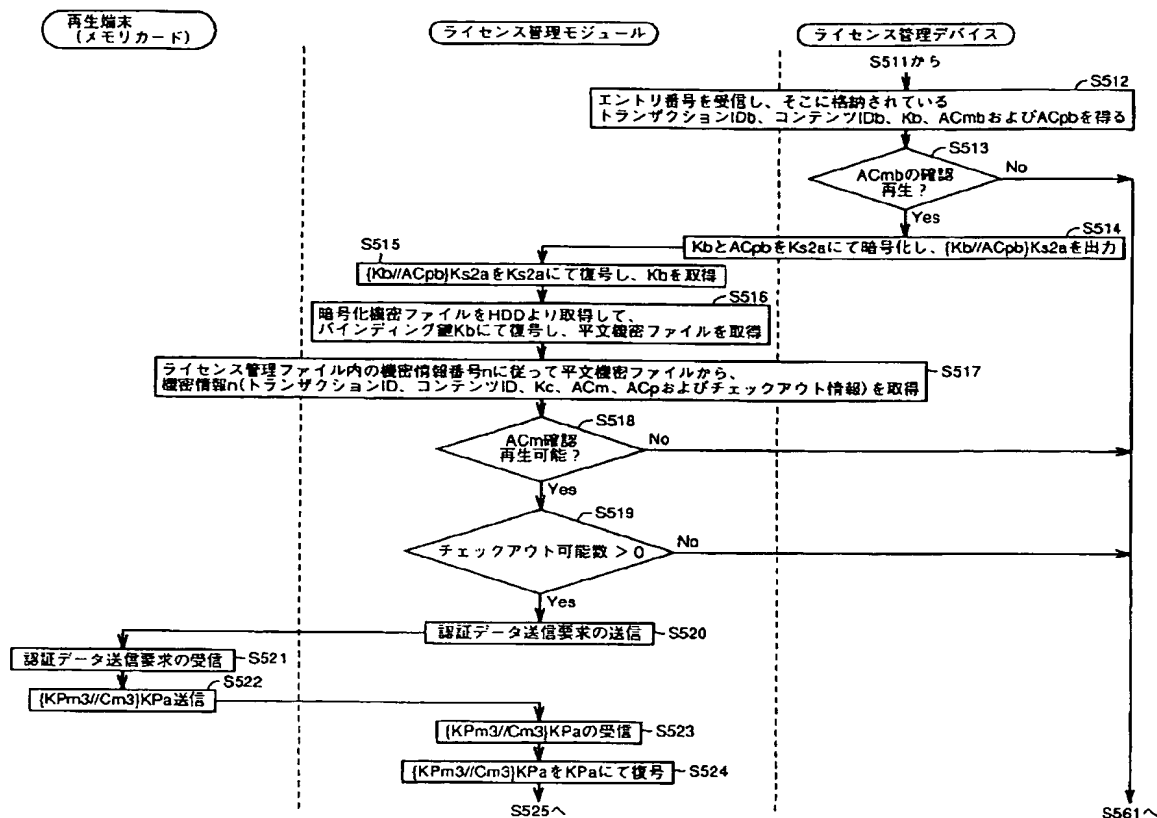
【図29】



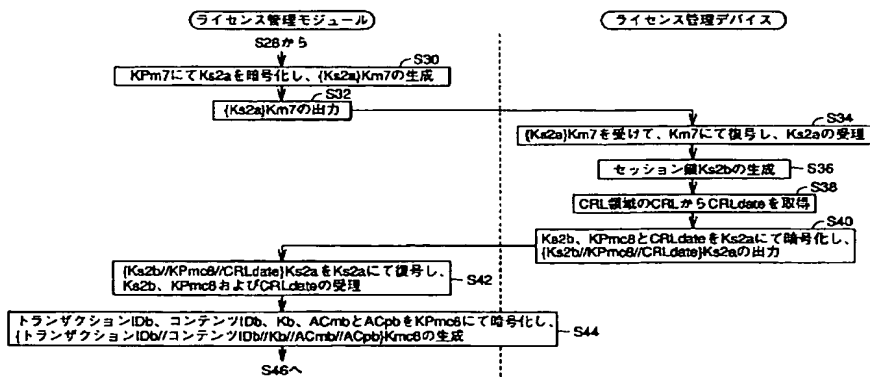
【図30】



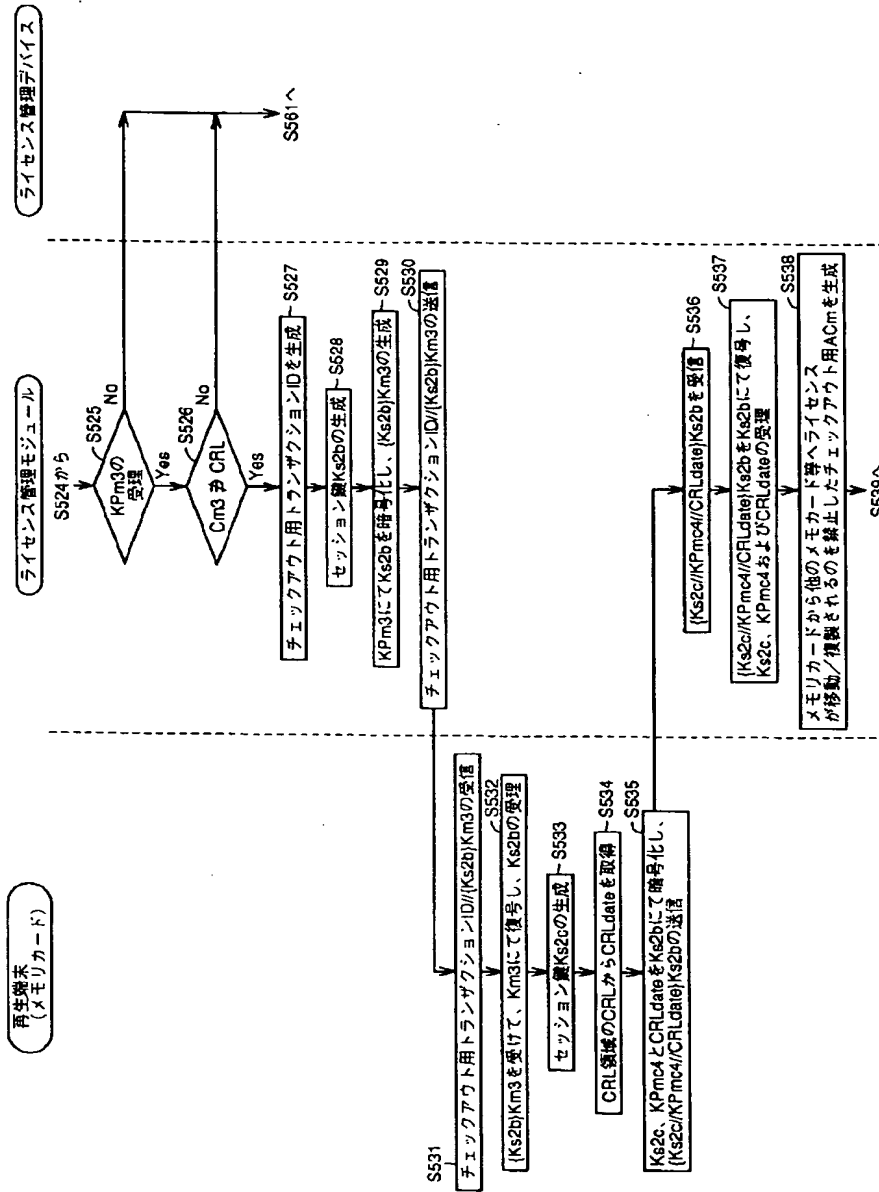
【図31】



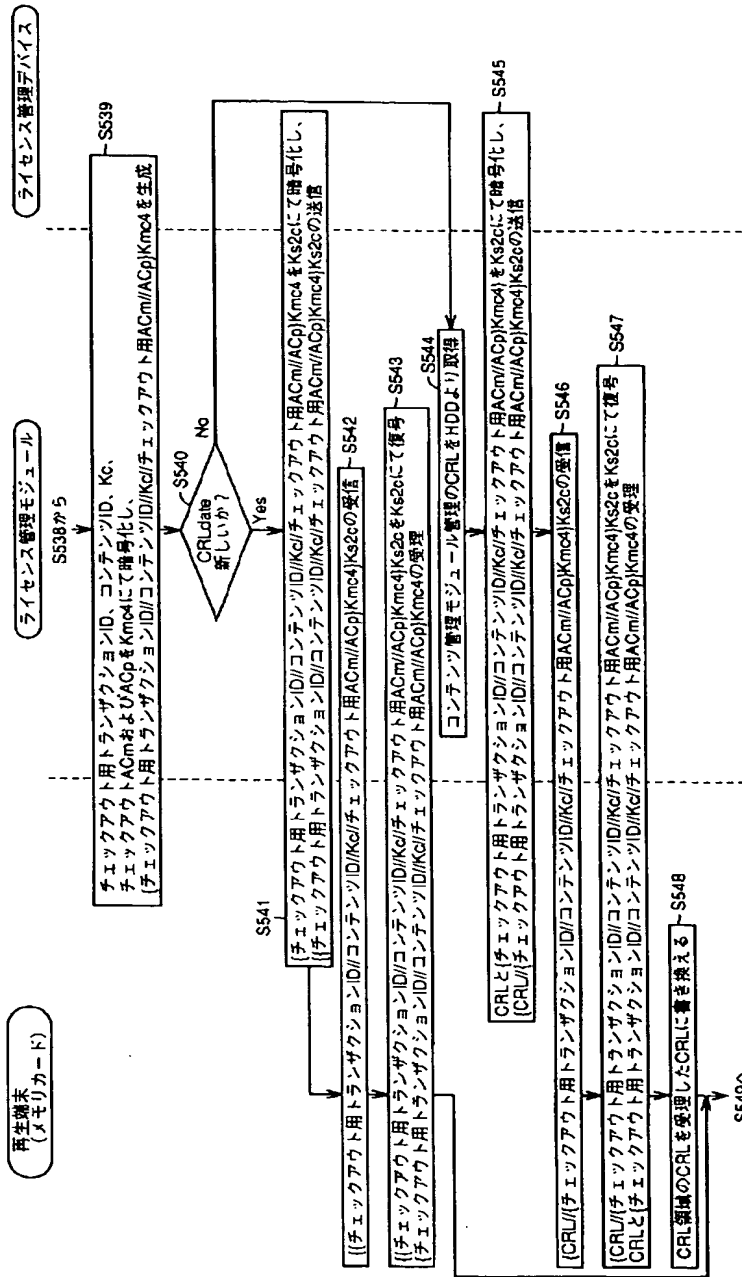
【図51】



【図32】

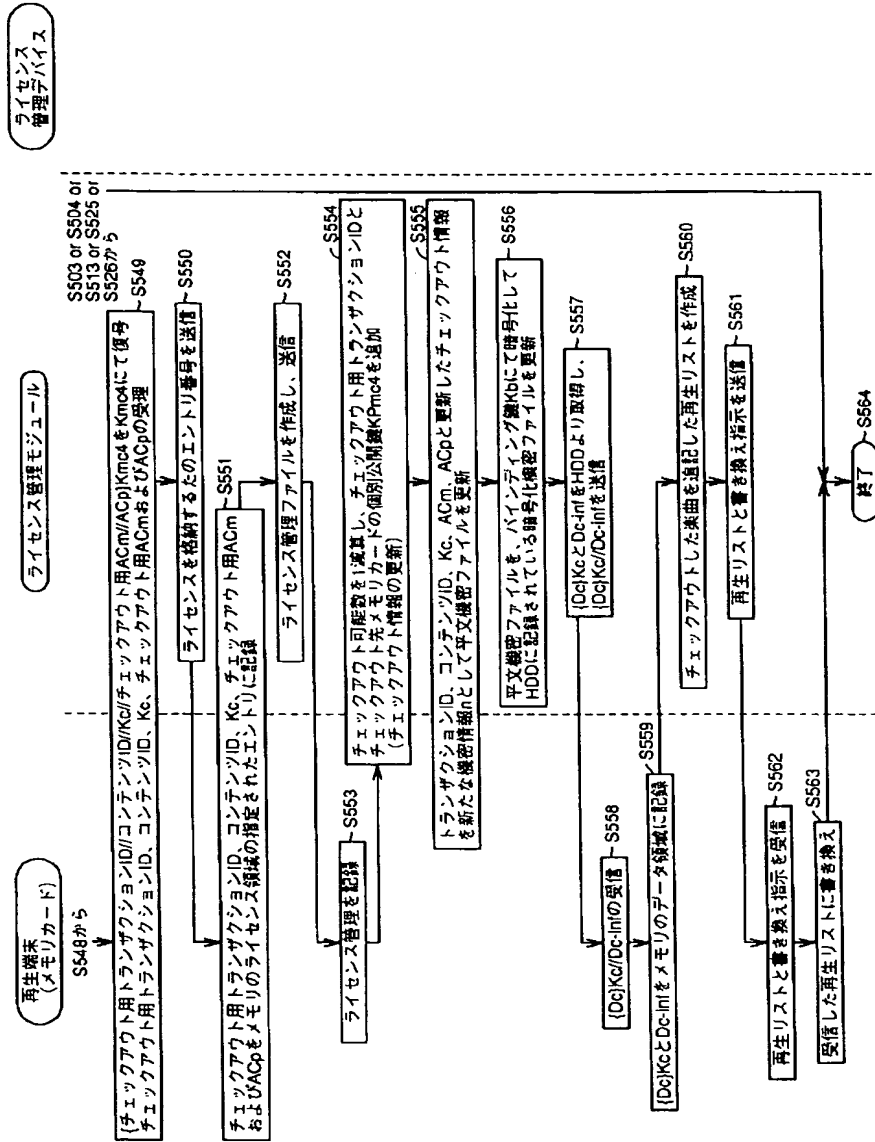


【図33】

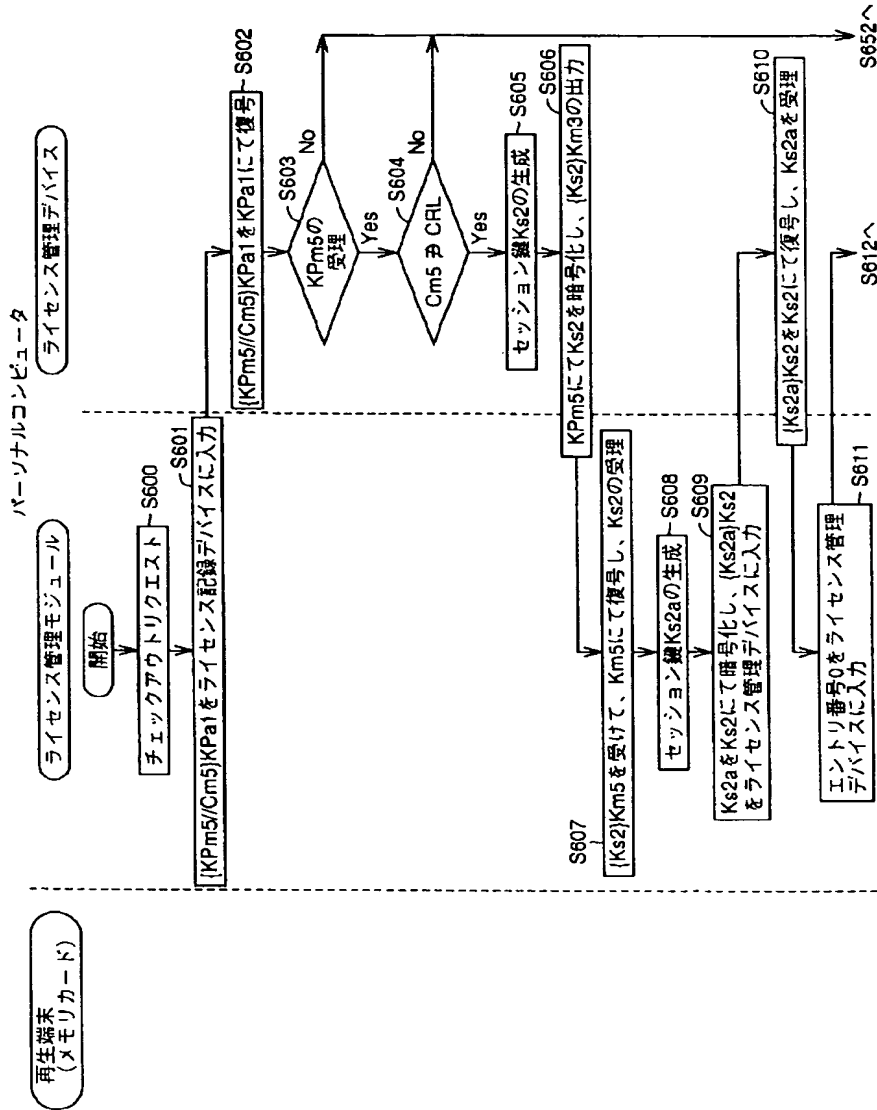




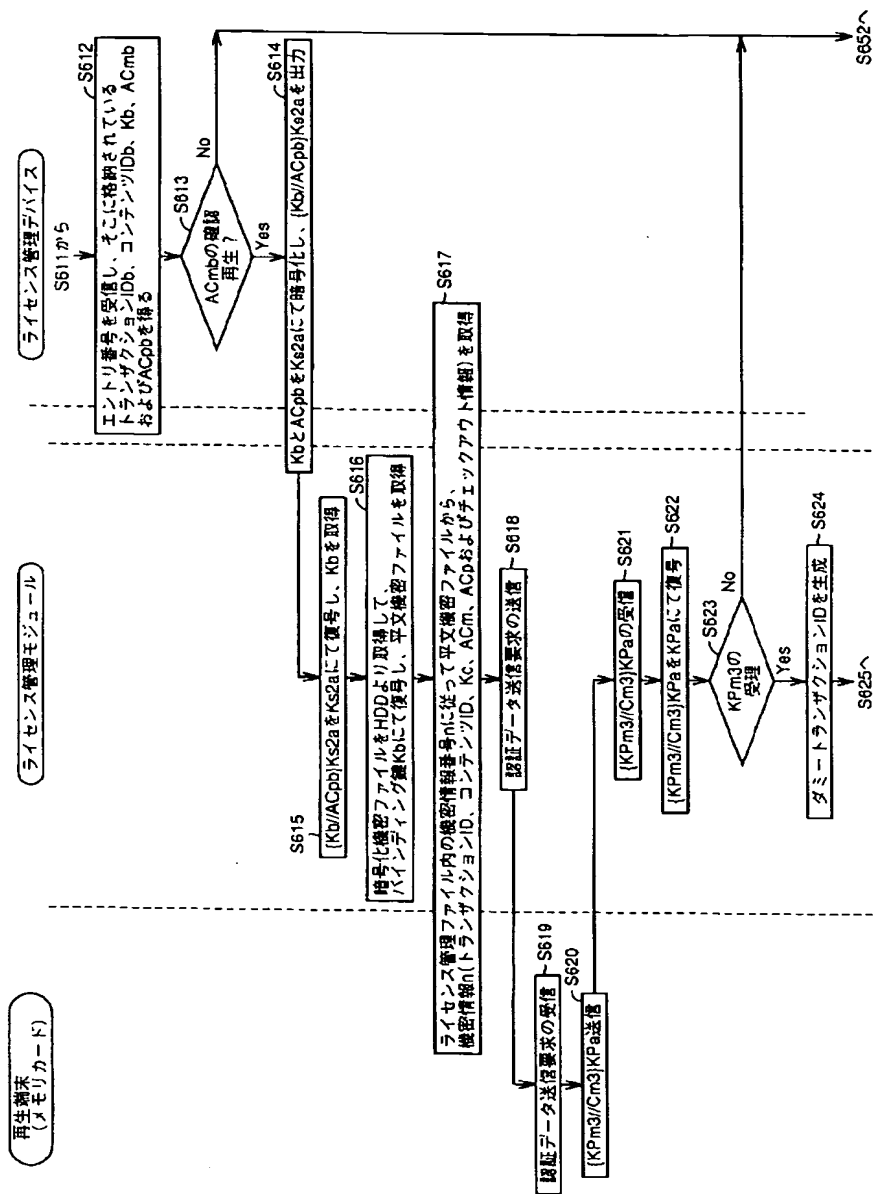
【図34】



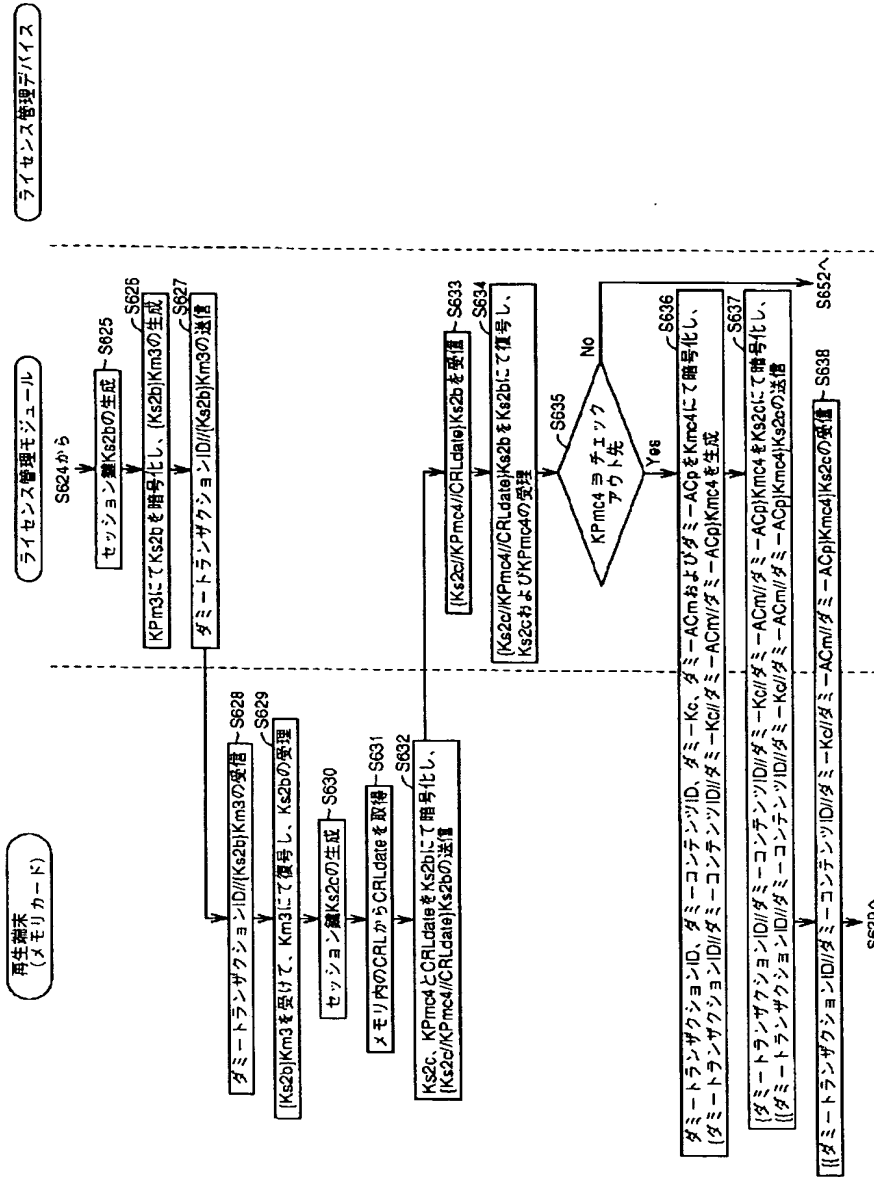
【図35】



【図36】

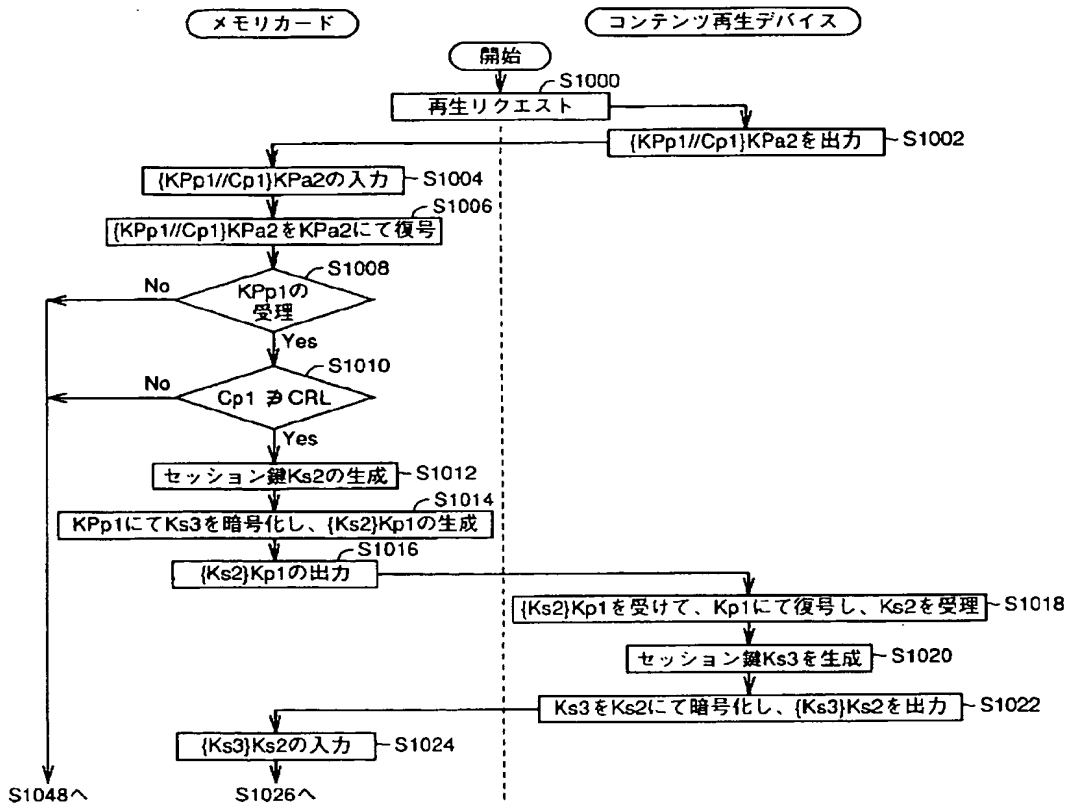


【図37】

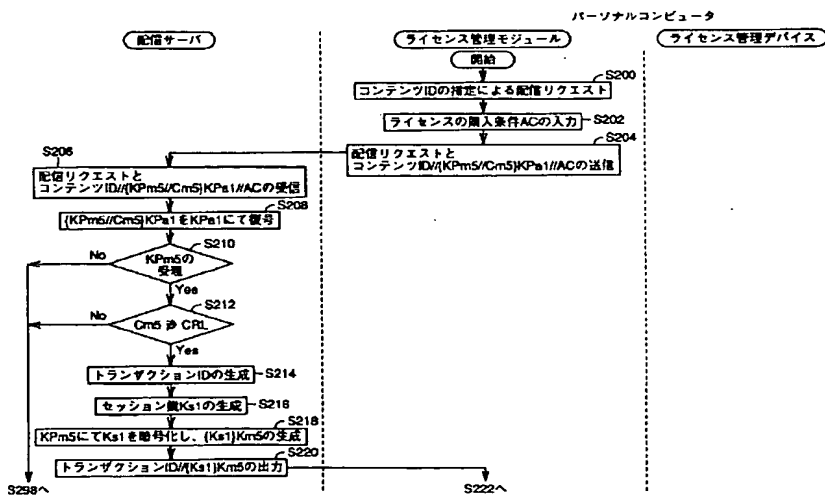




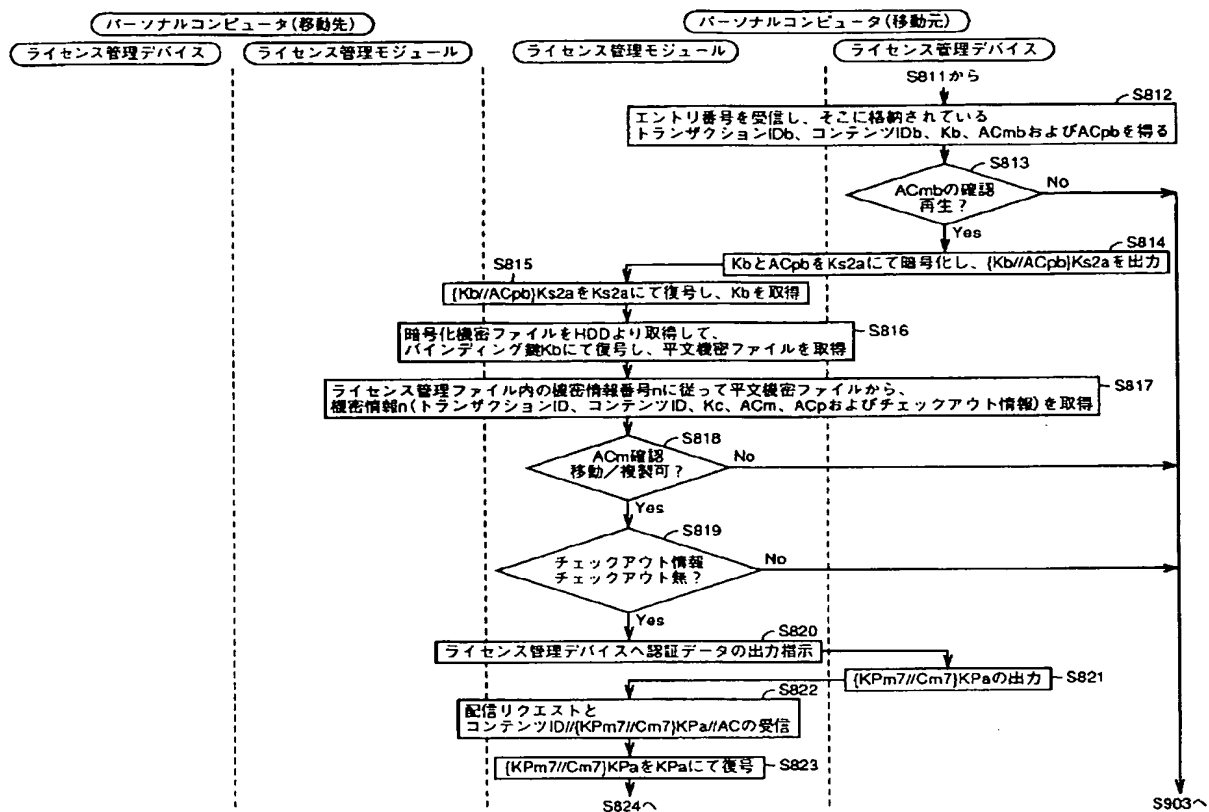
【図39】



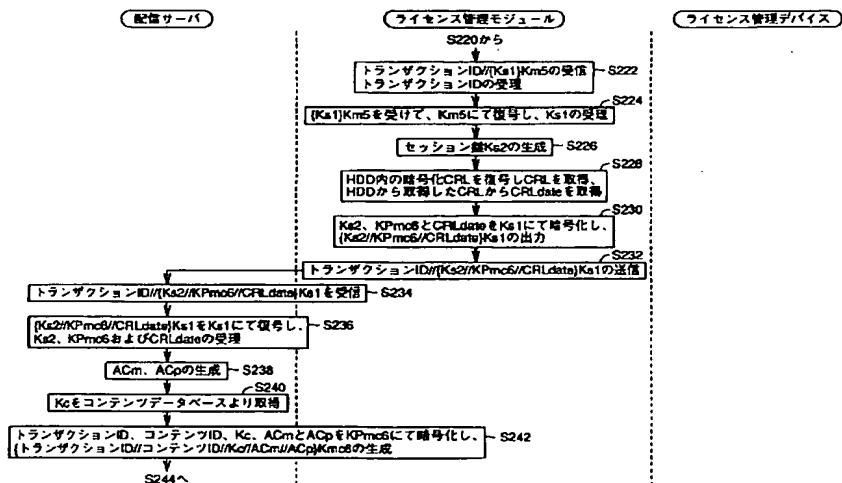
【図53】



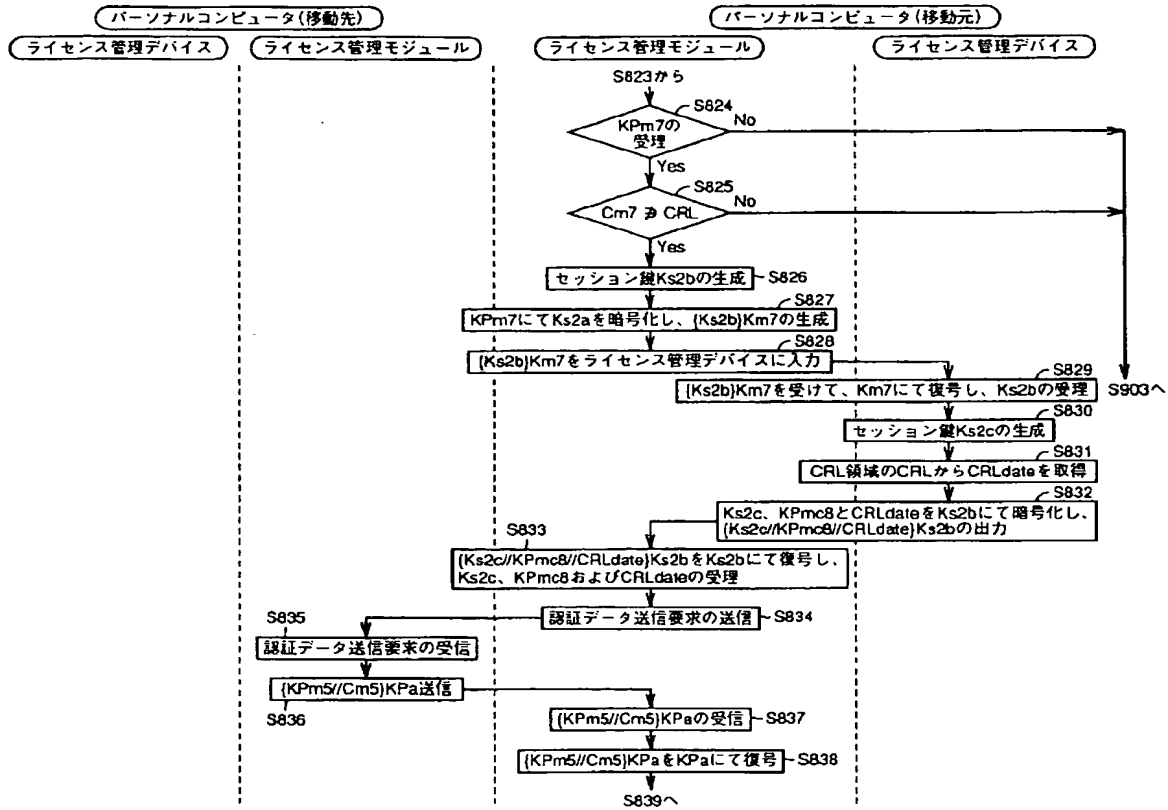
【図42】



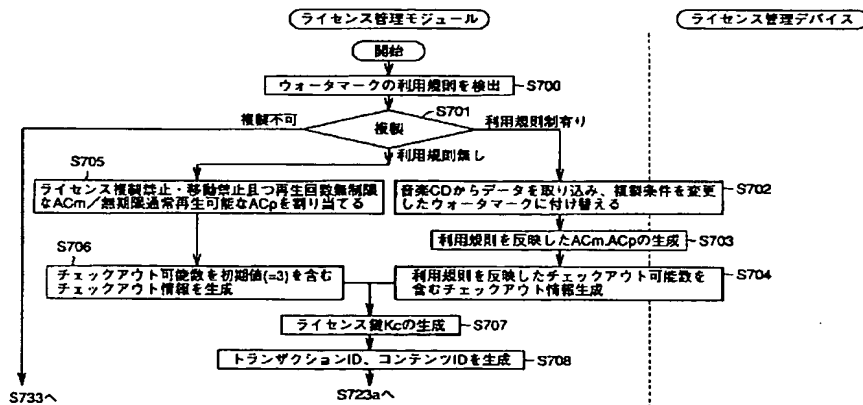
【図54】



【図43】

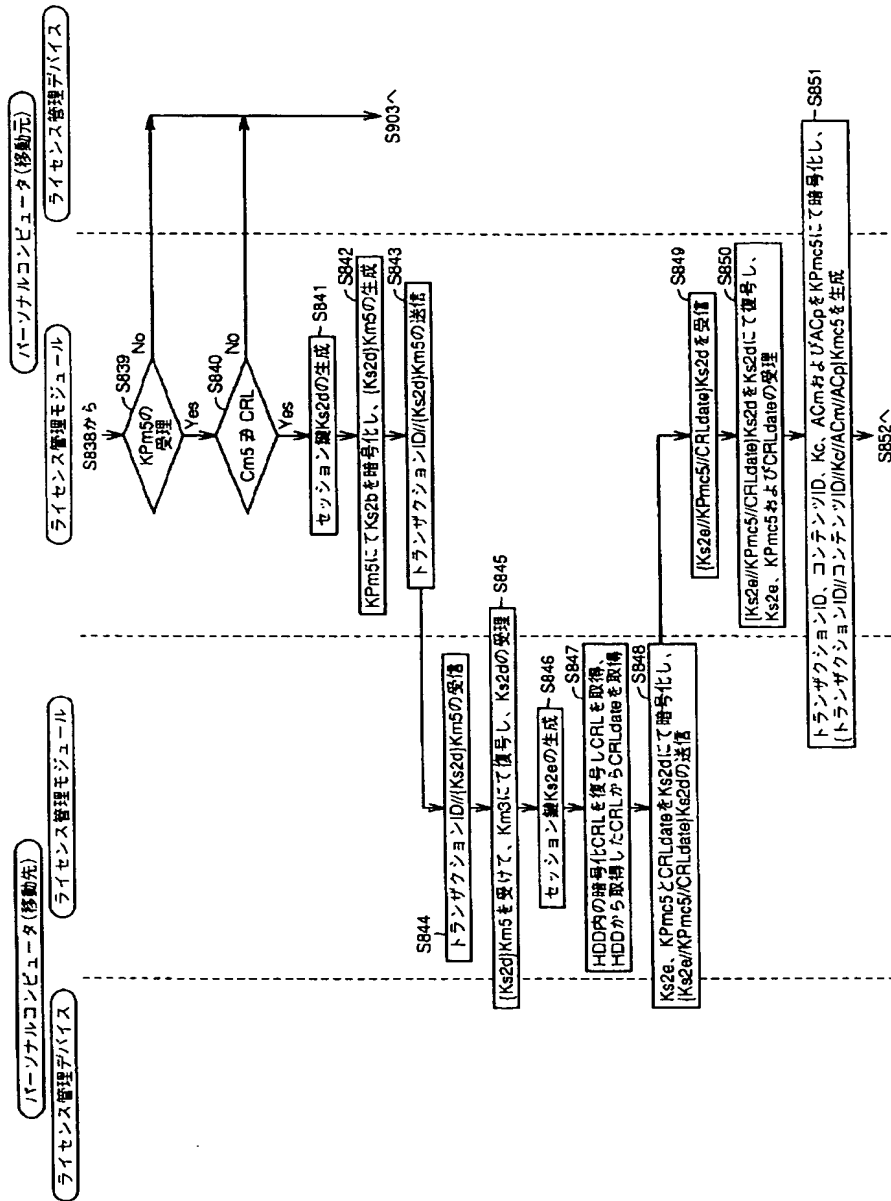


【図57】

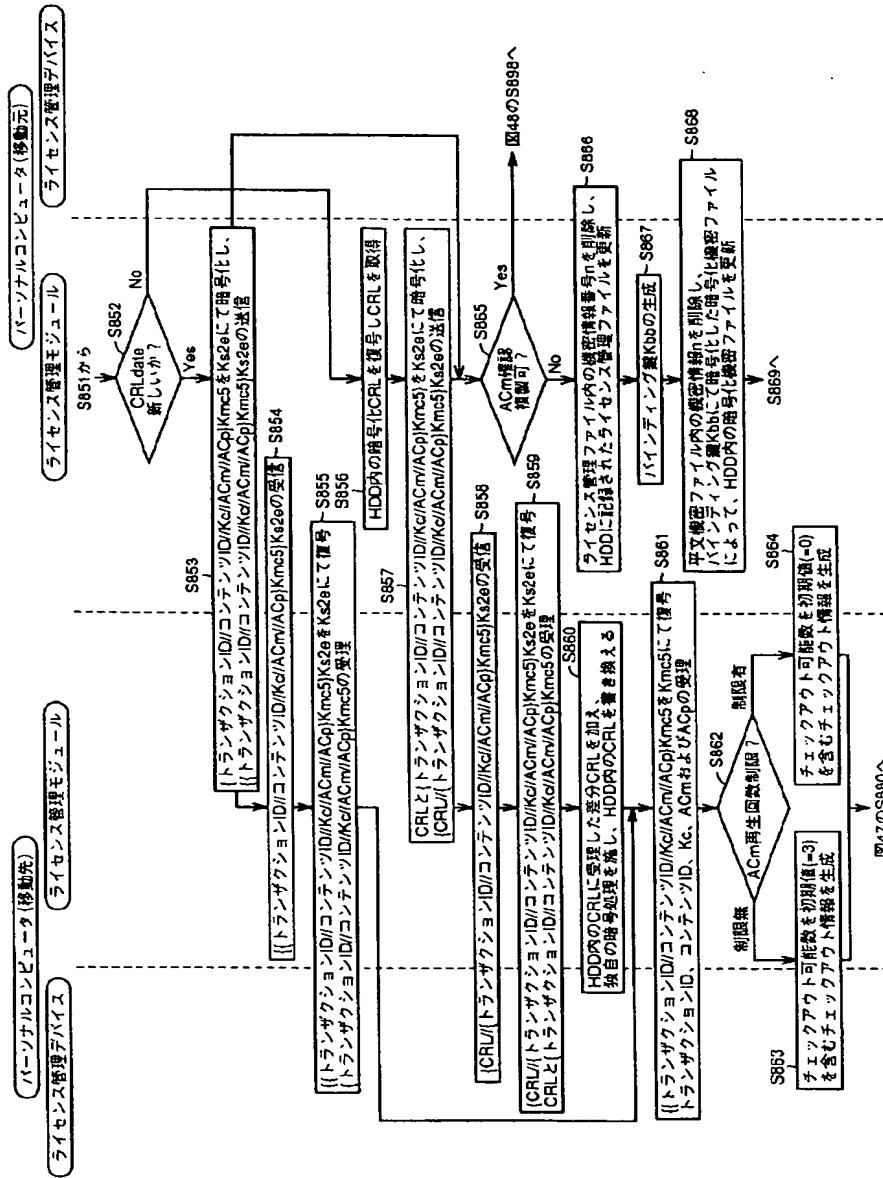




【図44】



【図45】



【図46】

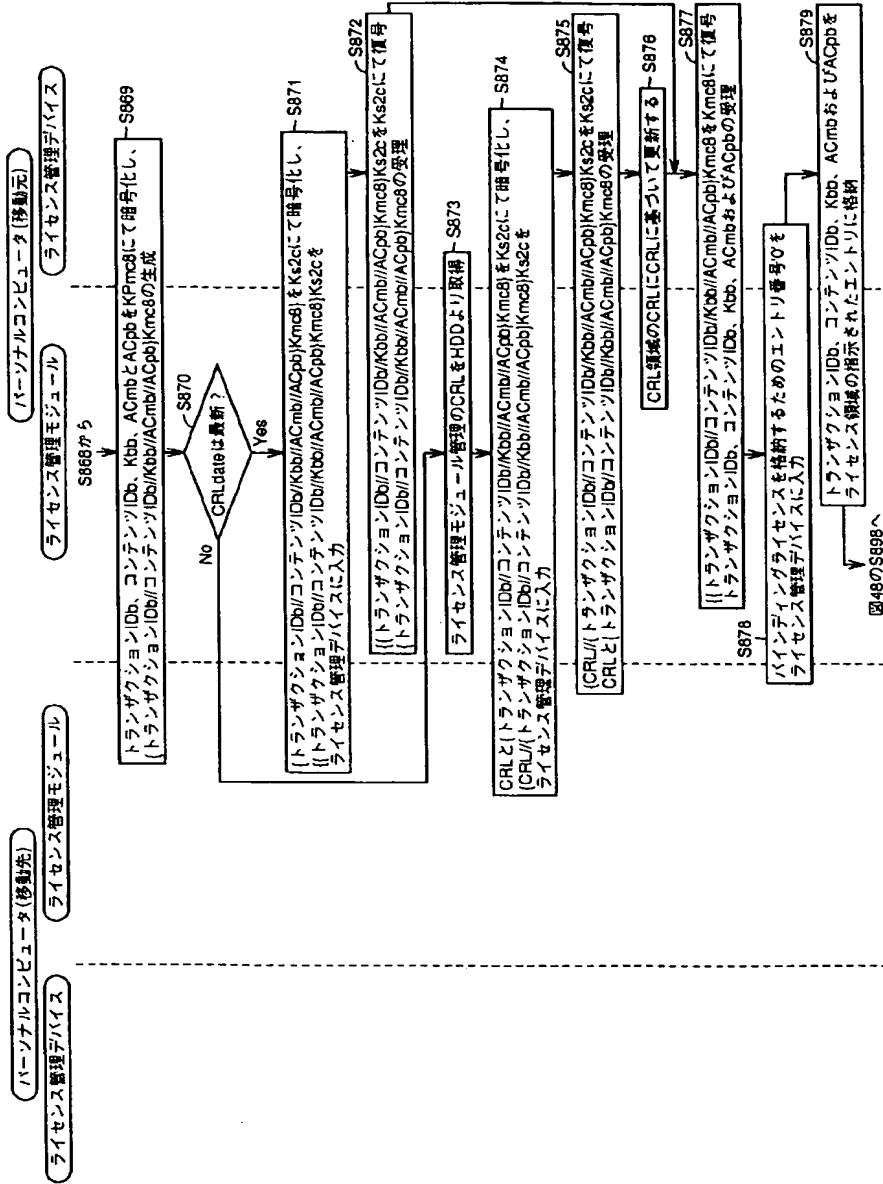
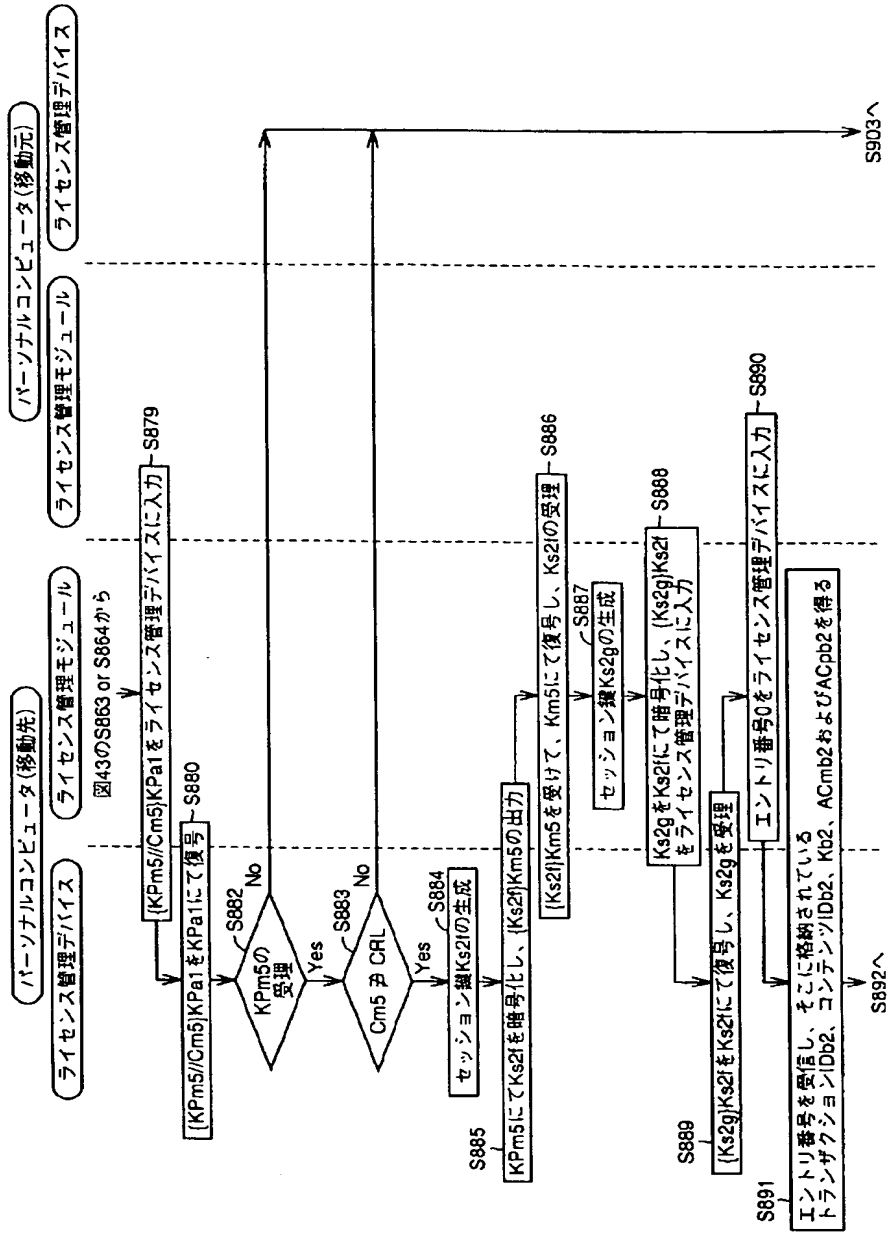
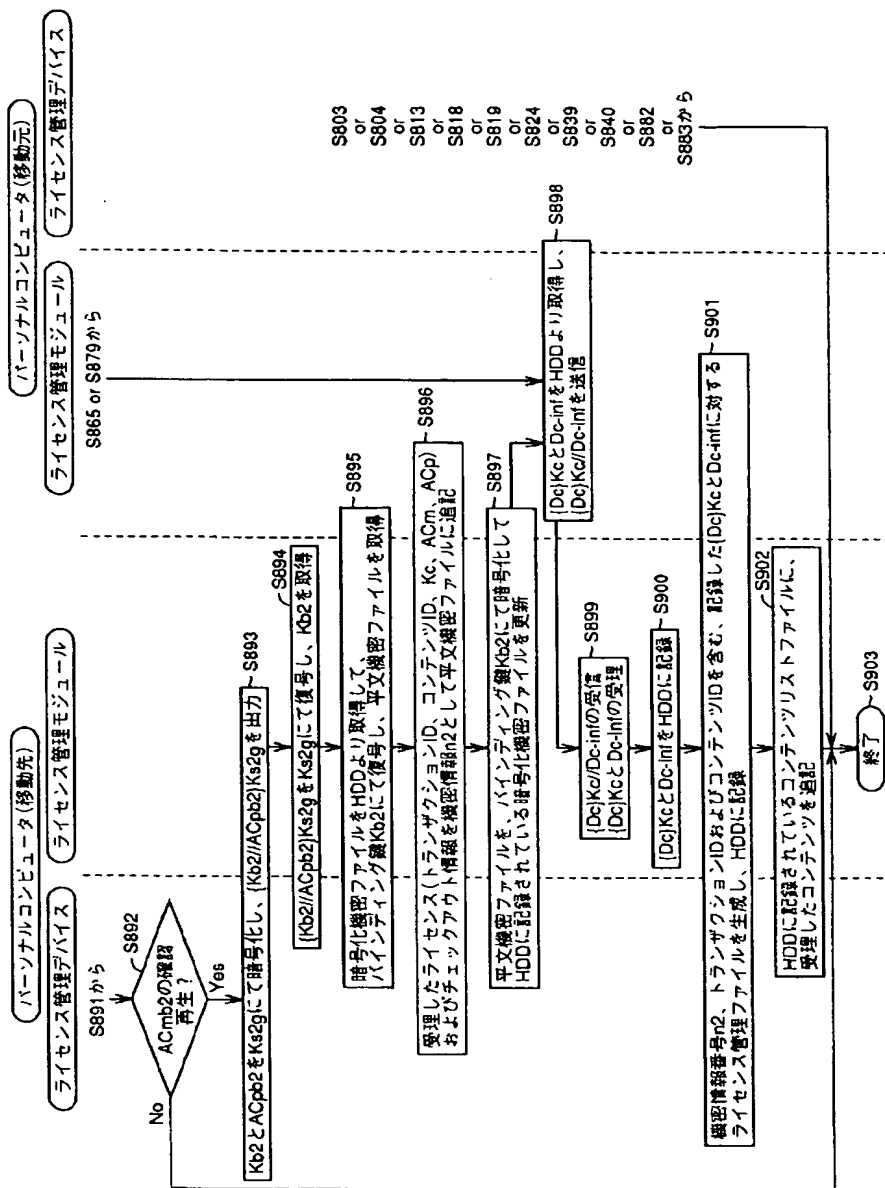


図48のS8198へ

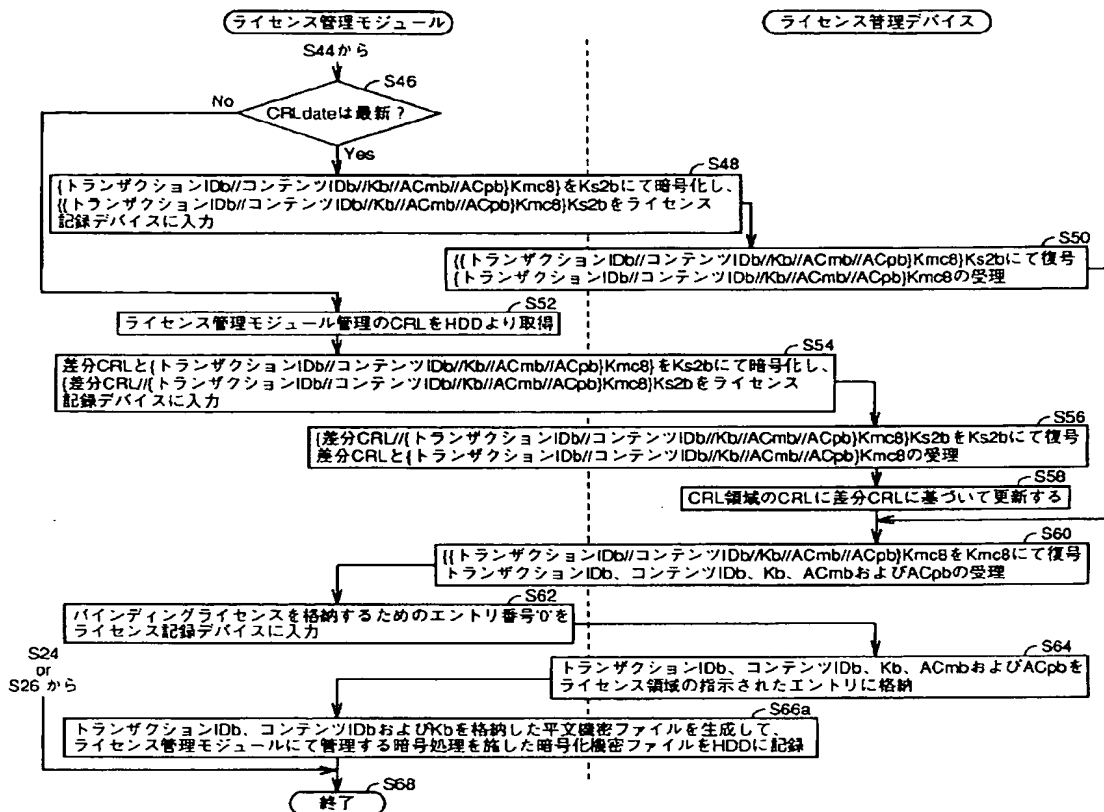
【図47】



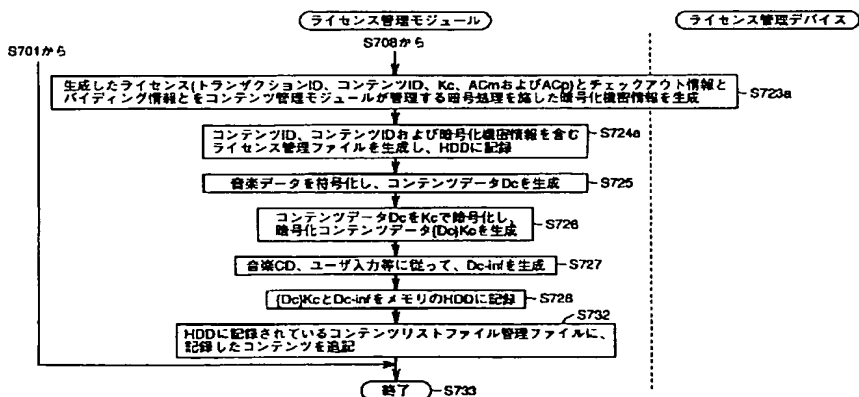
【図48】



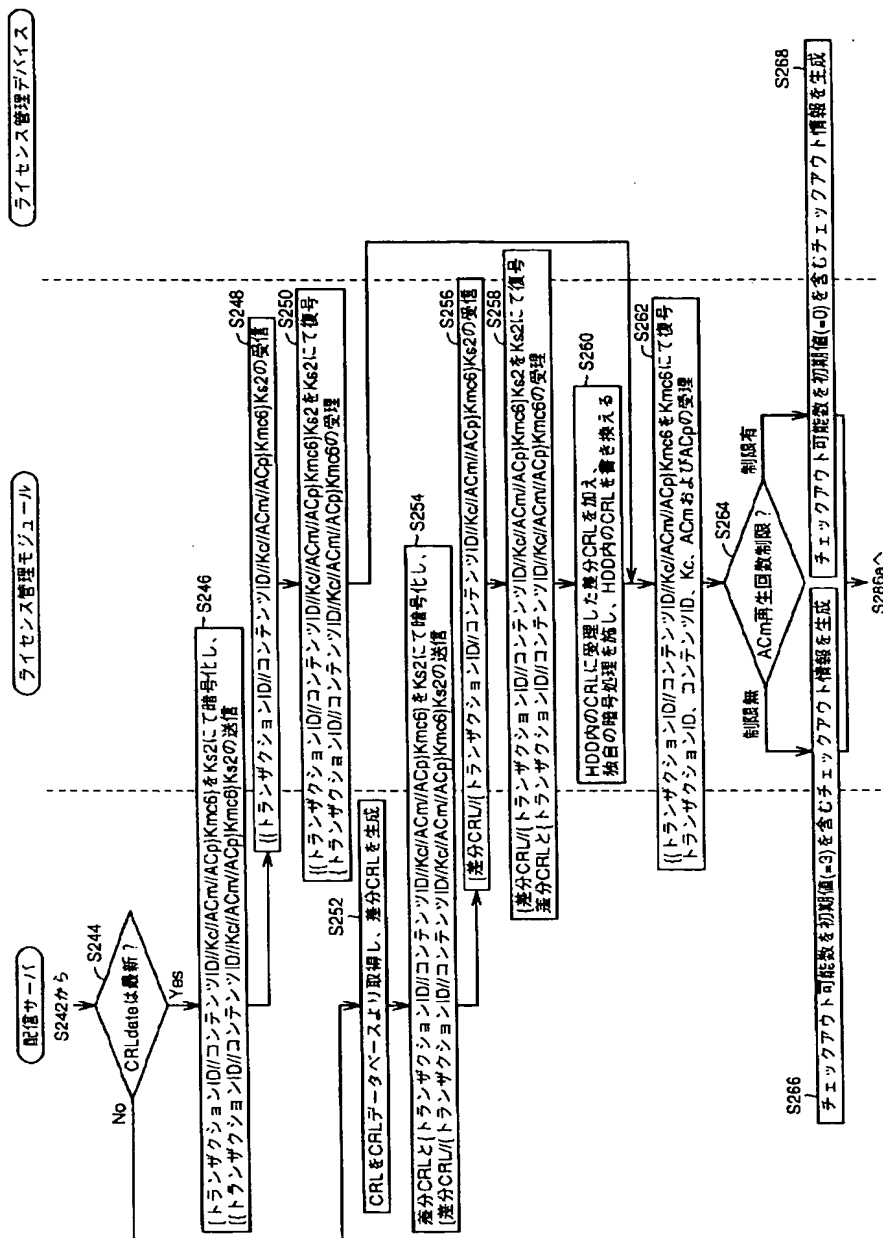
【図52】



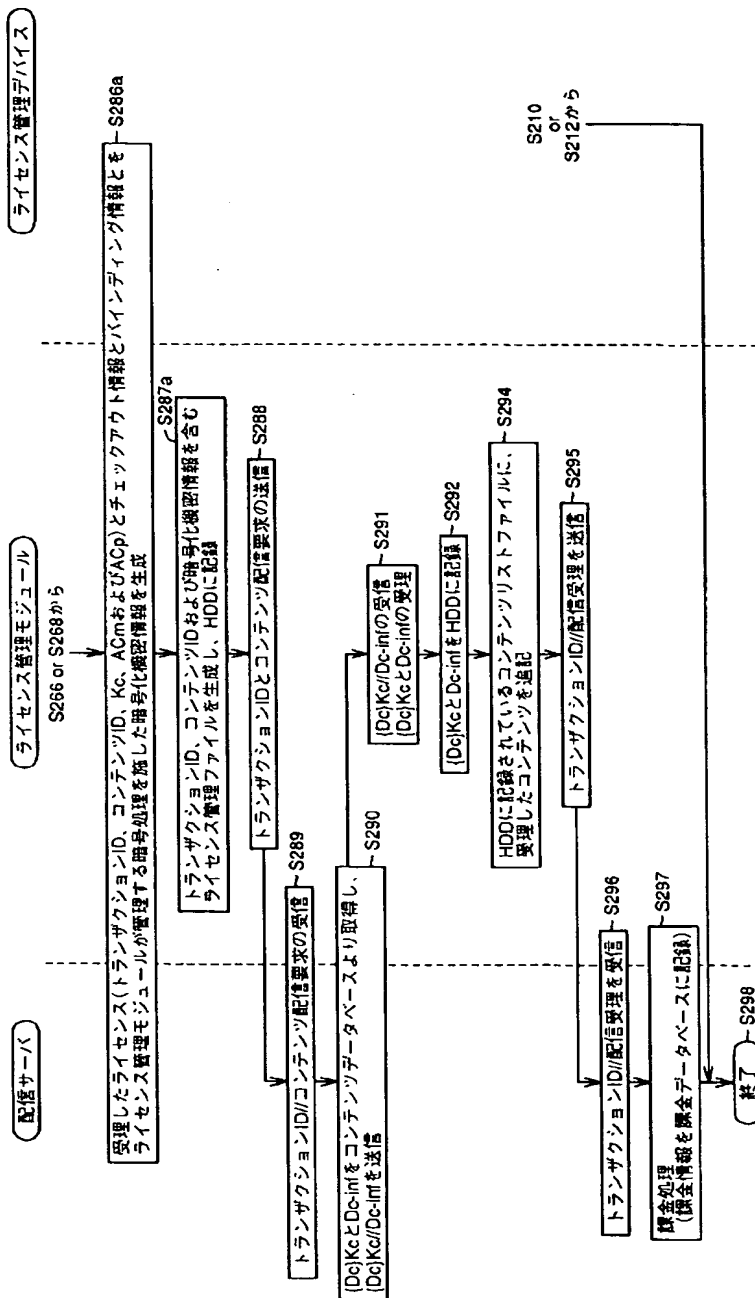
【図58】



【図55】

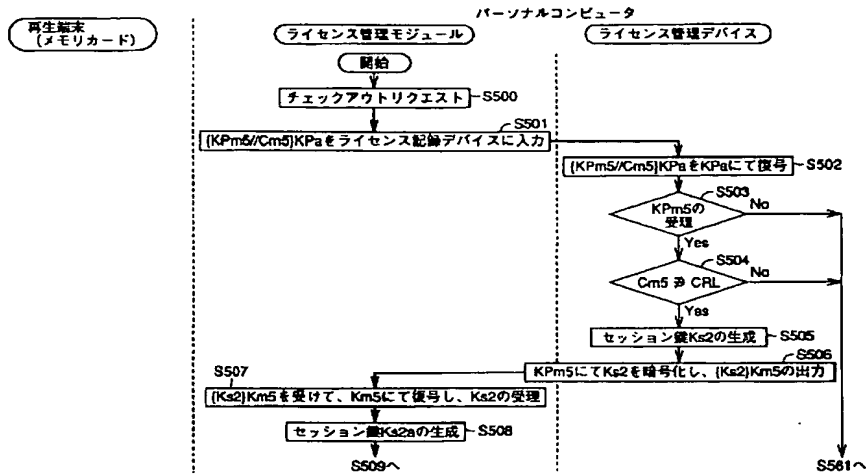


【図56】

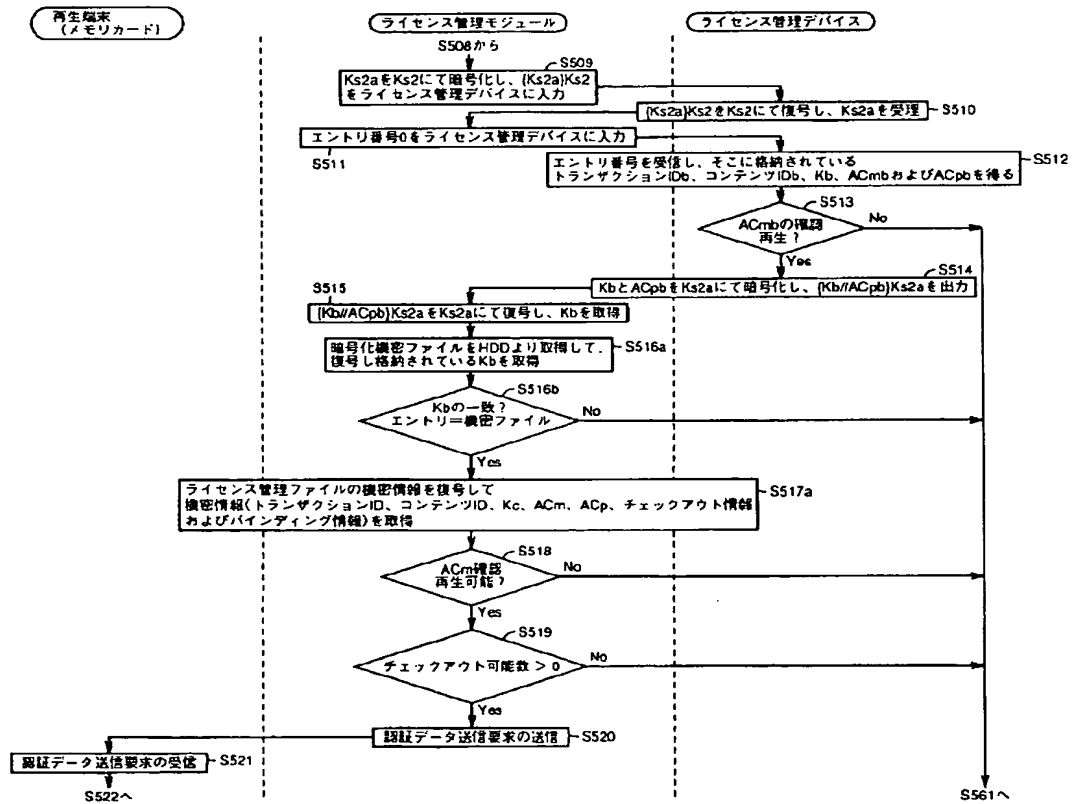




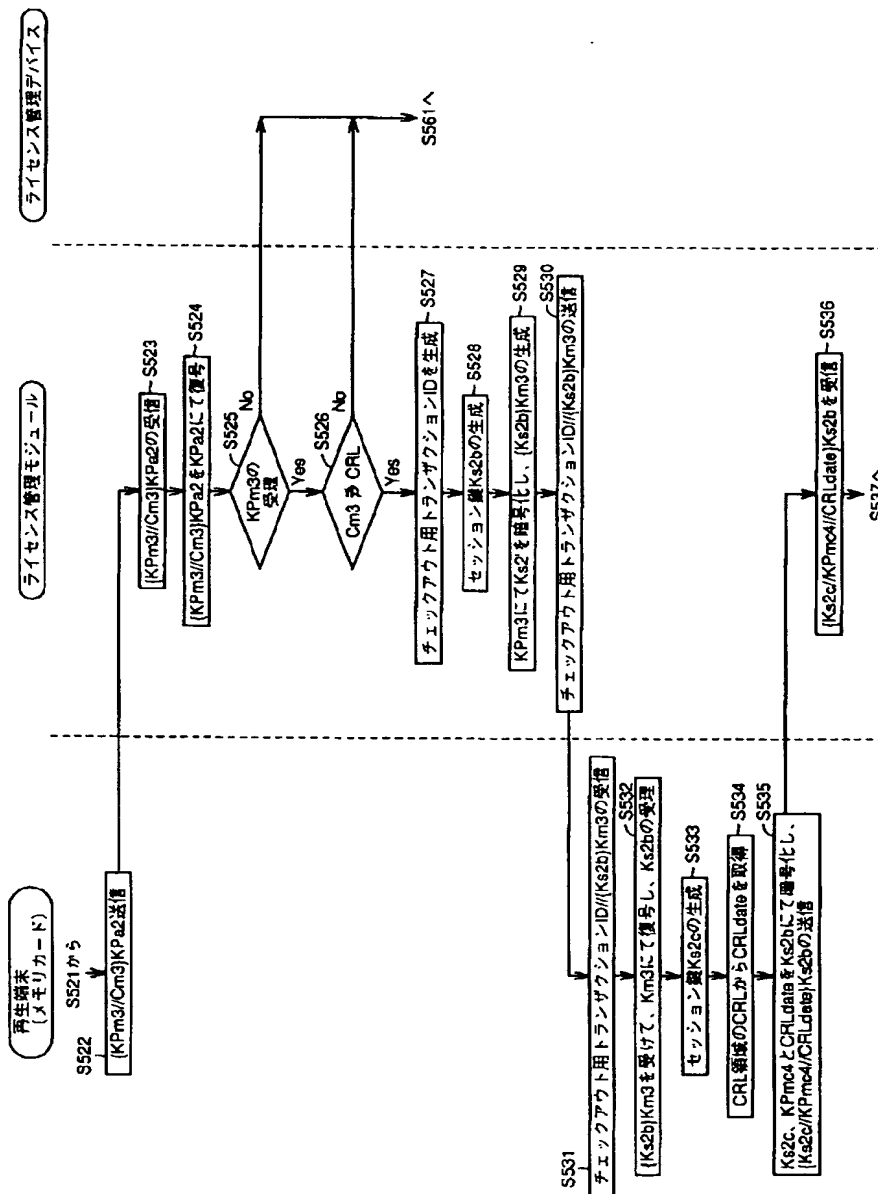
【図59】



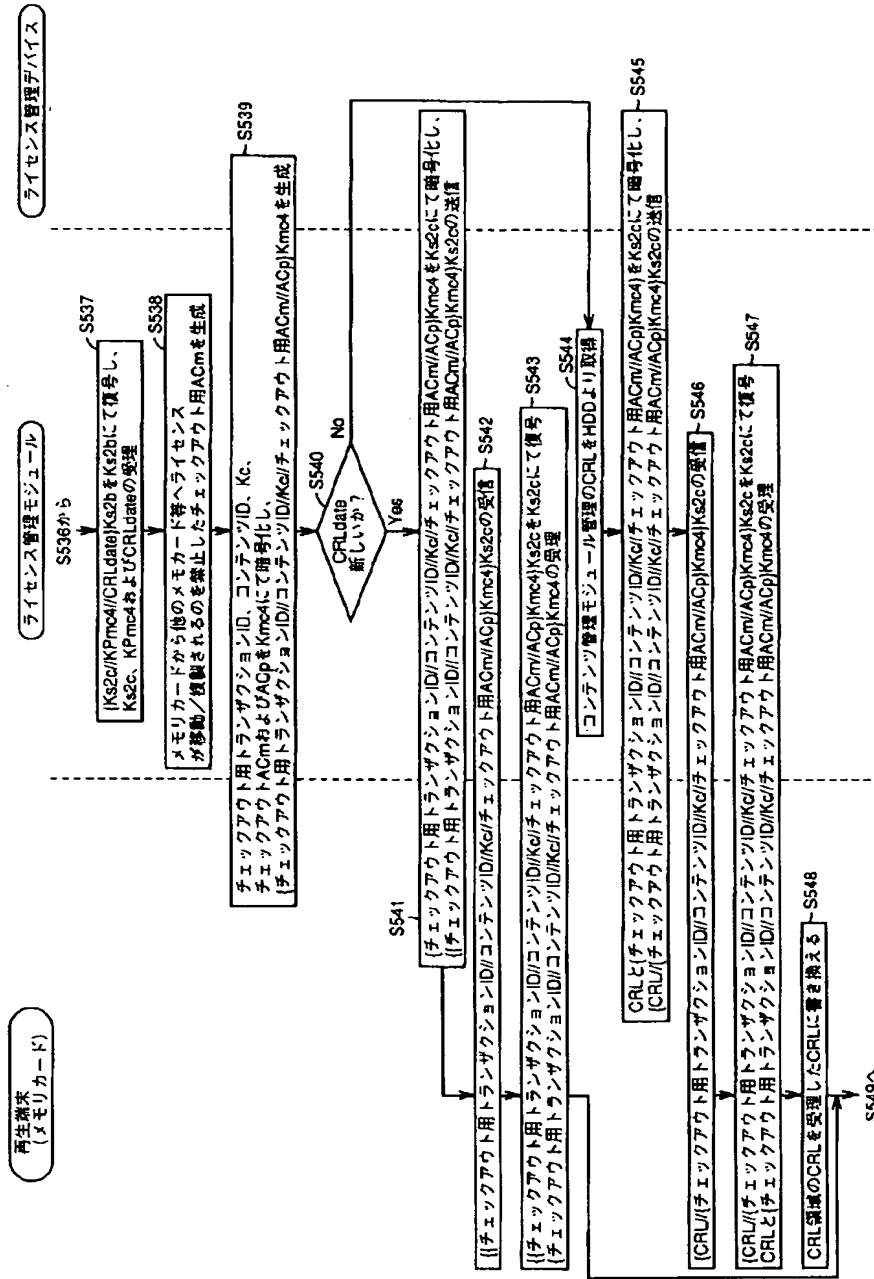
【図60】



【図61】

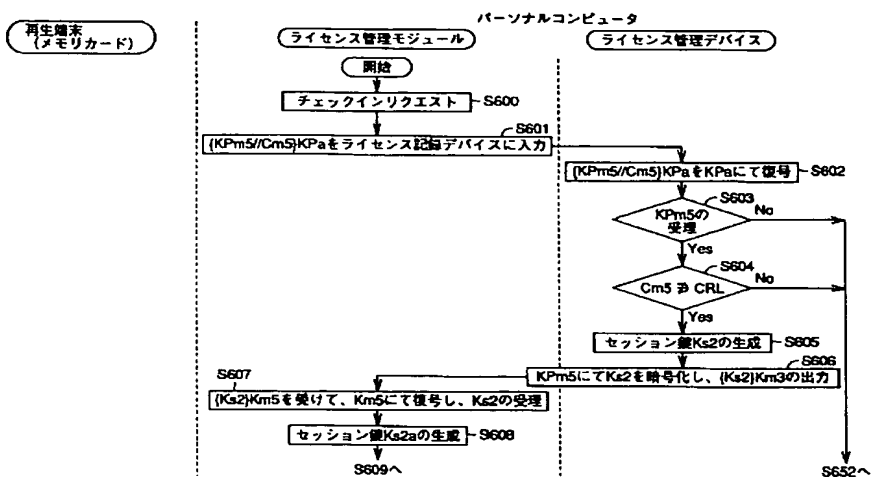


【図 62】

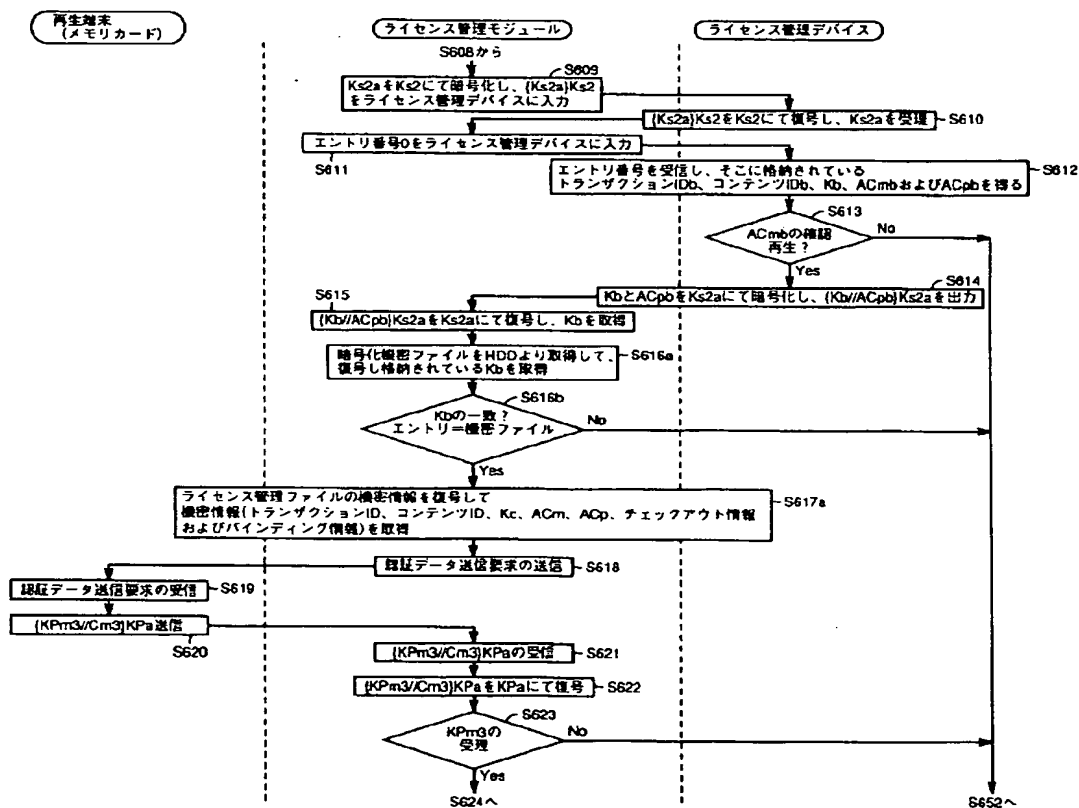




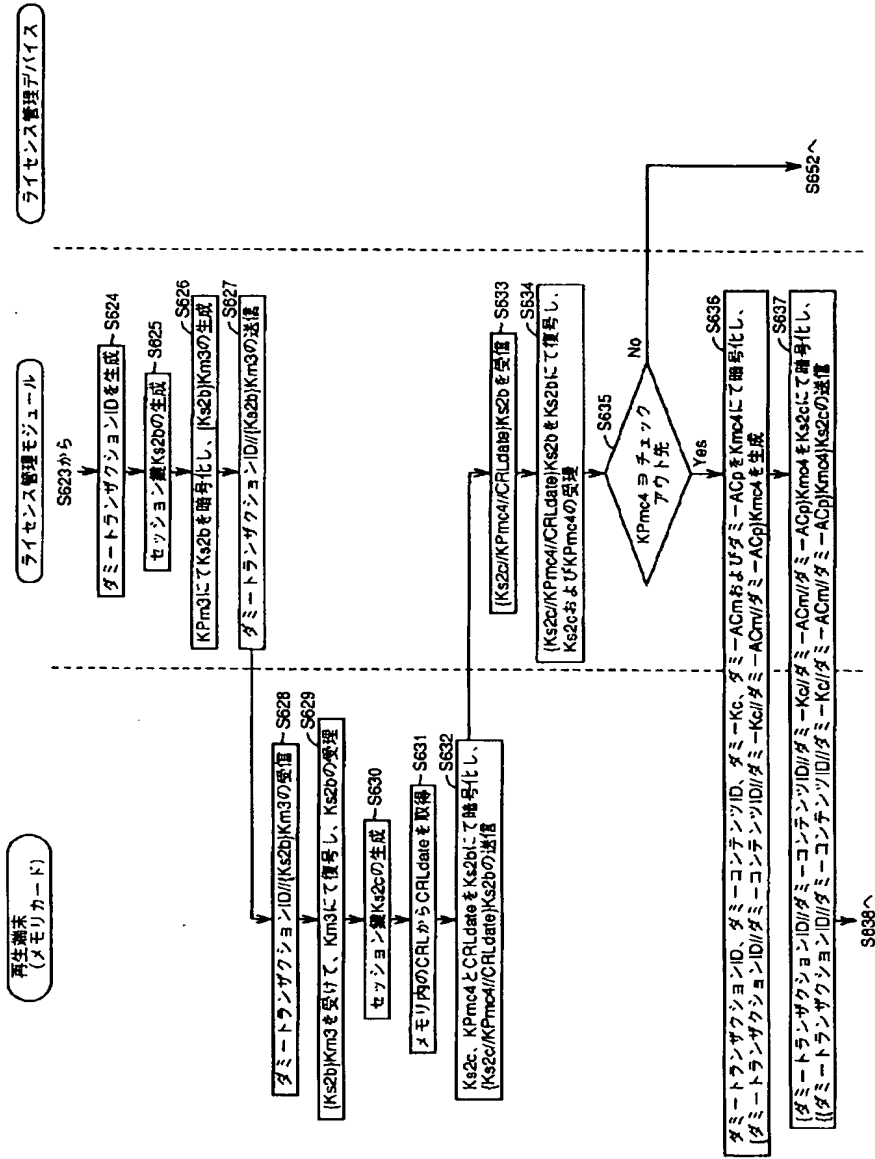
【図64】



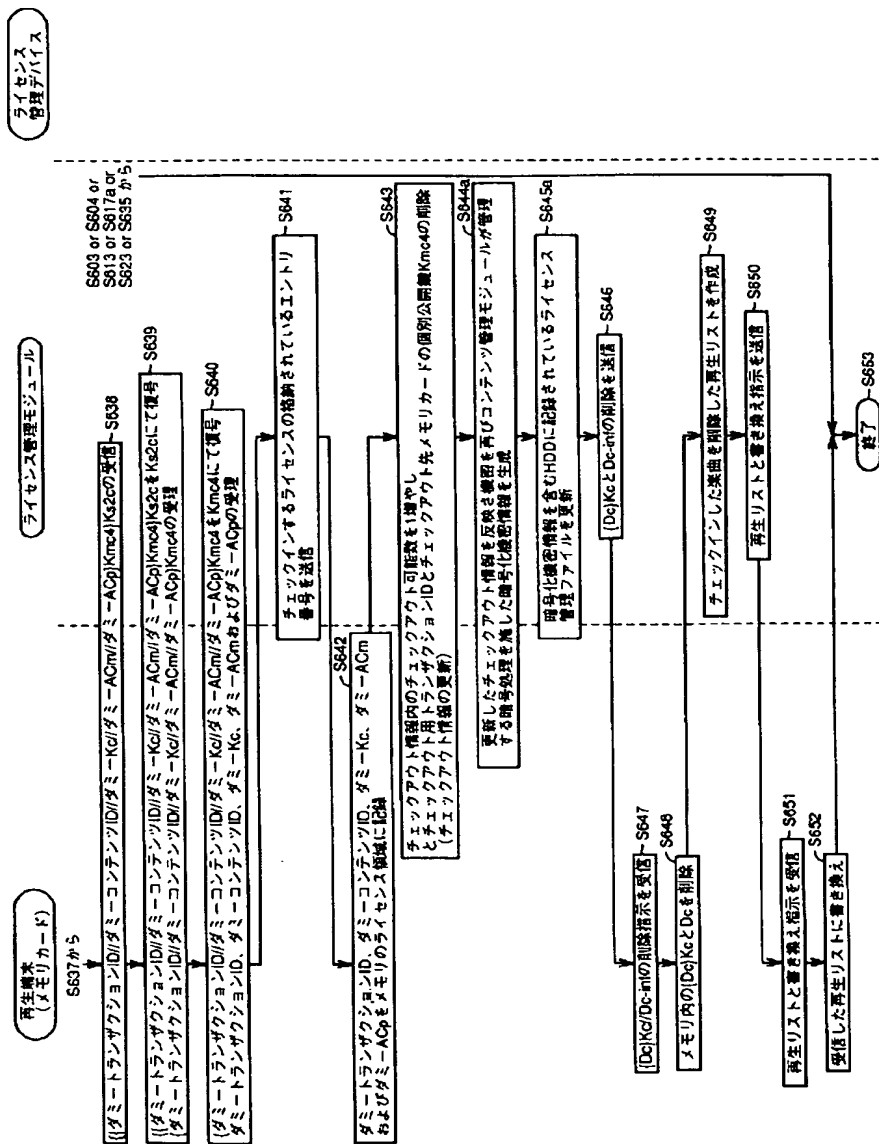
【図65】



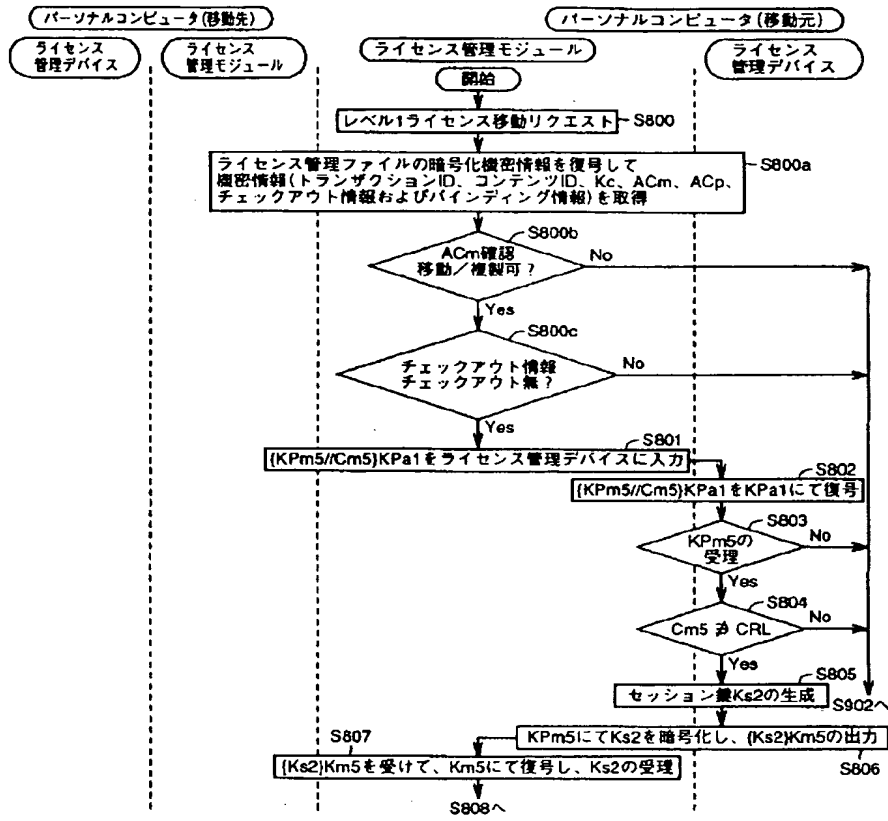
【図66】



【図67】

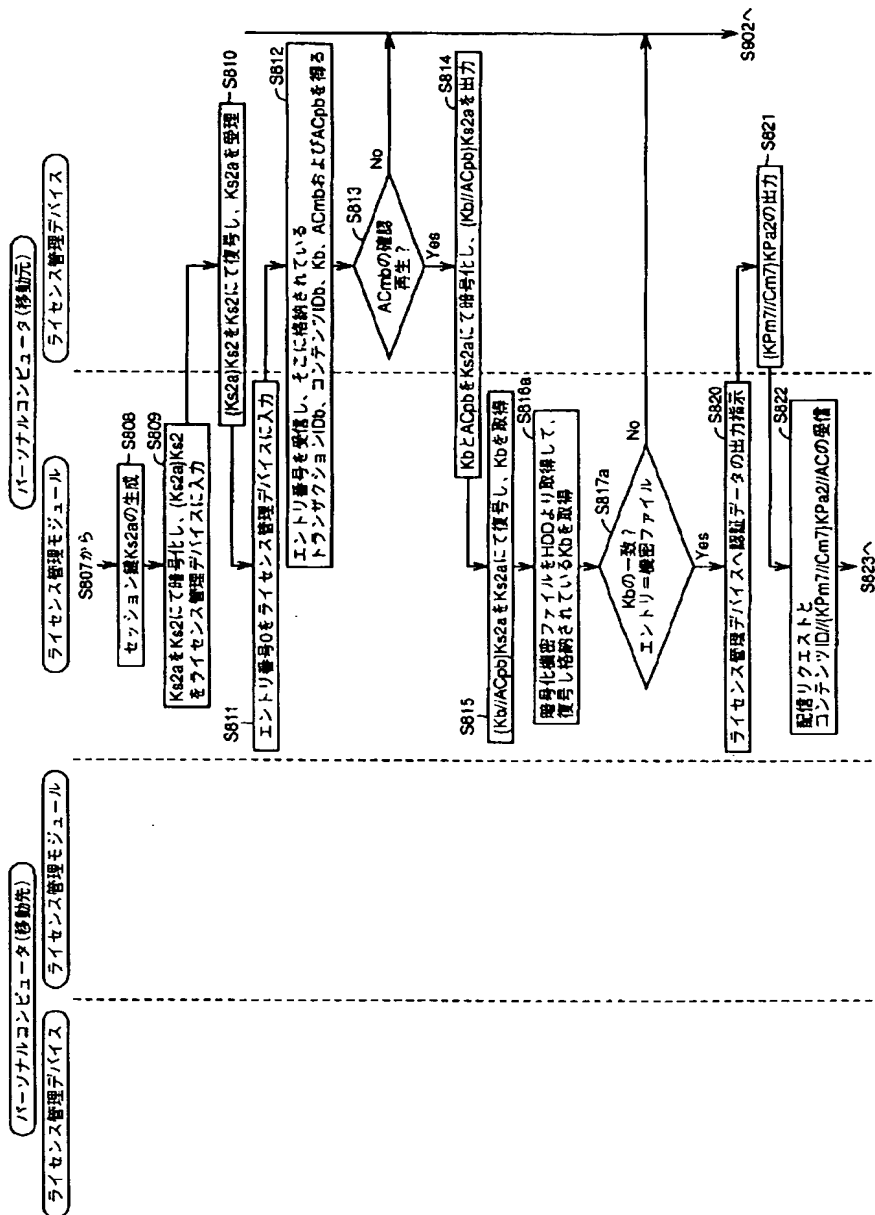


【図68】

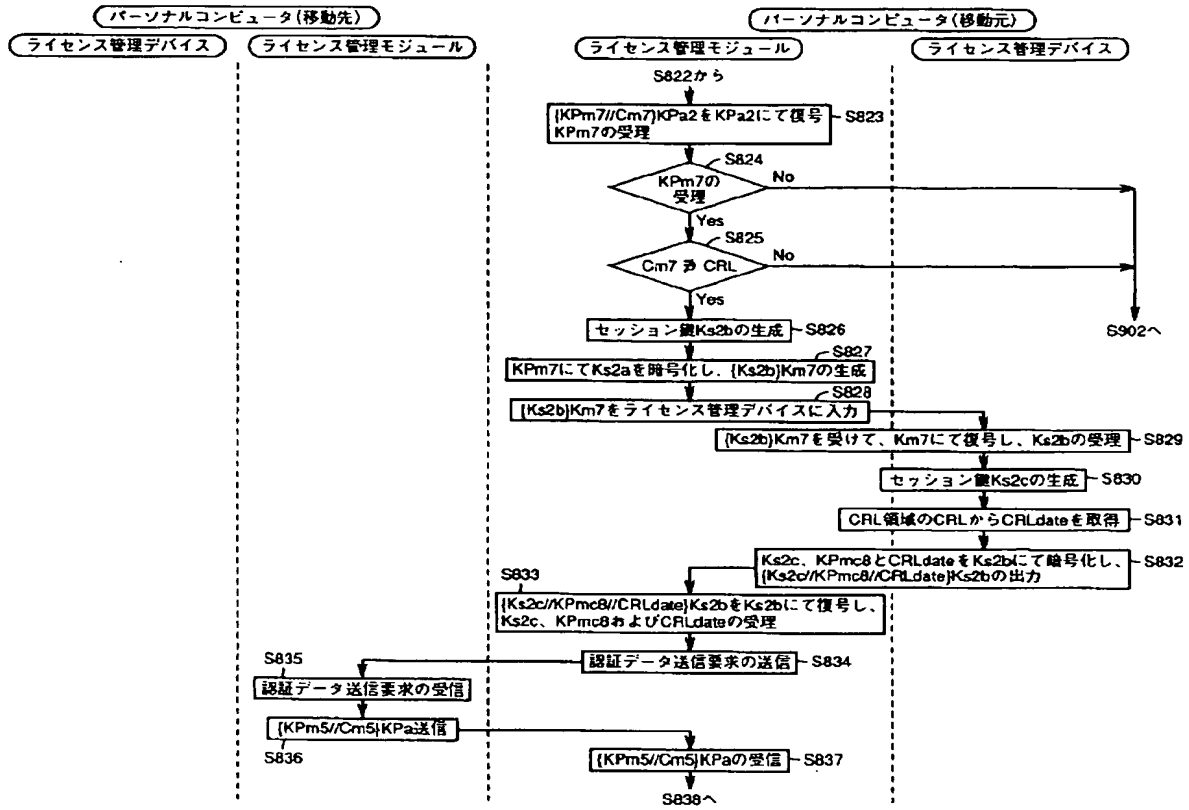




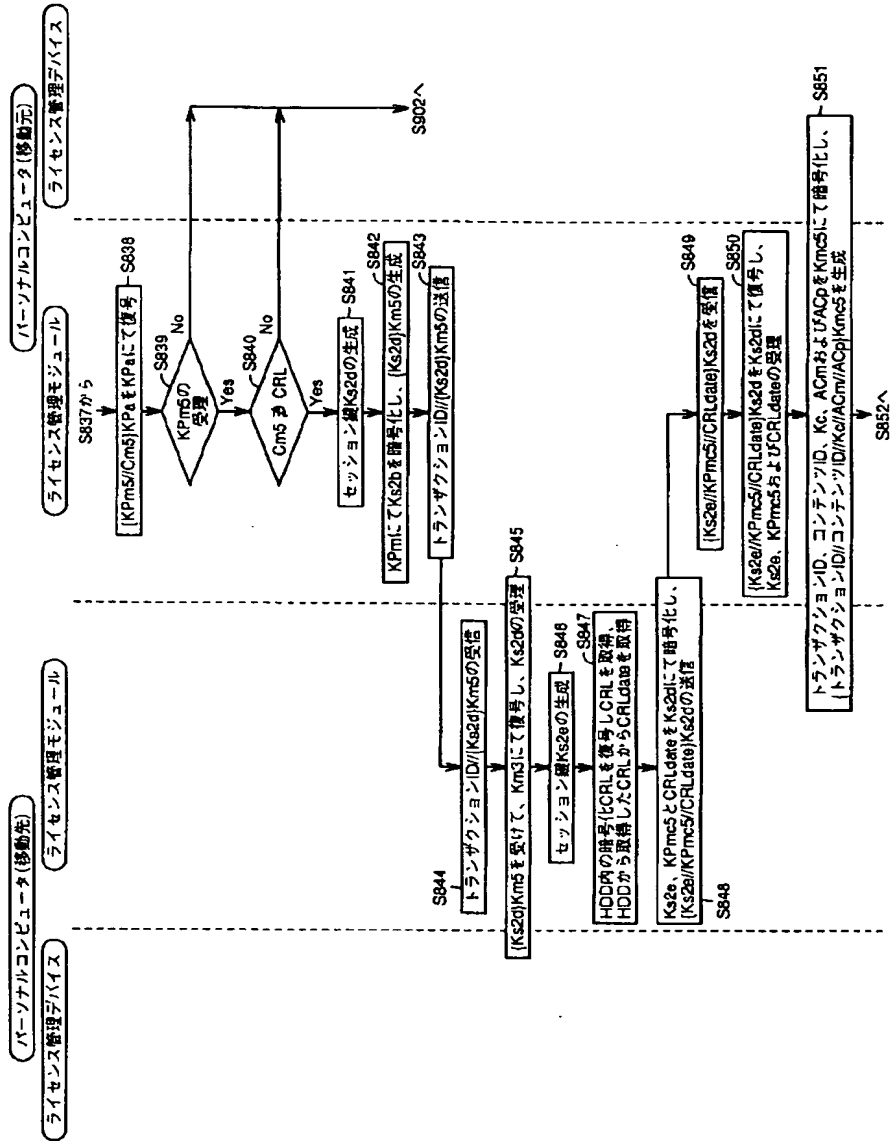
【図69】



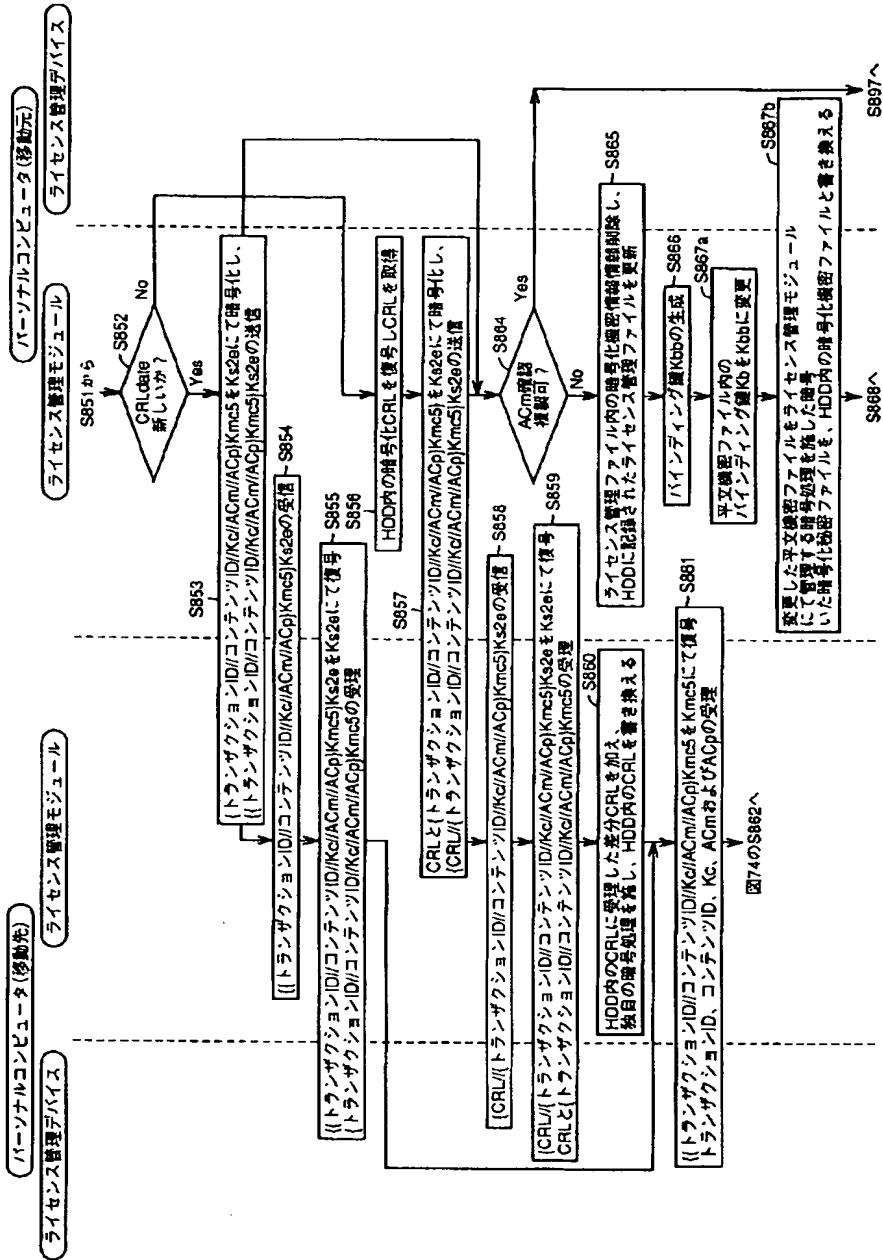
【図70】



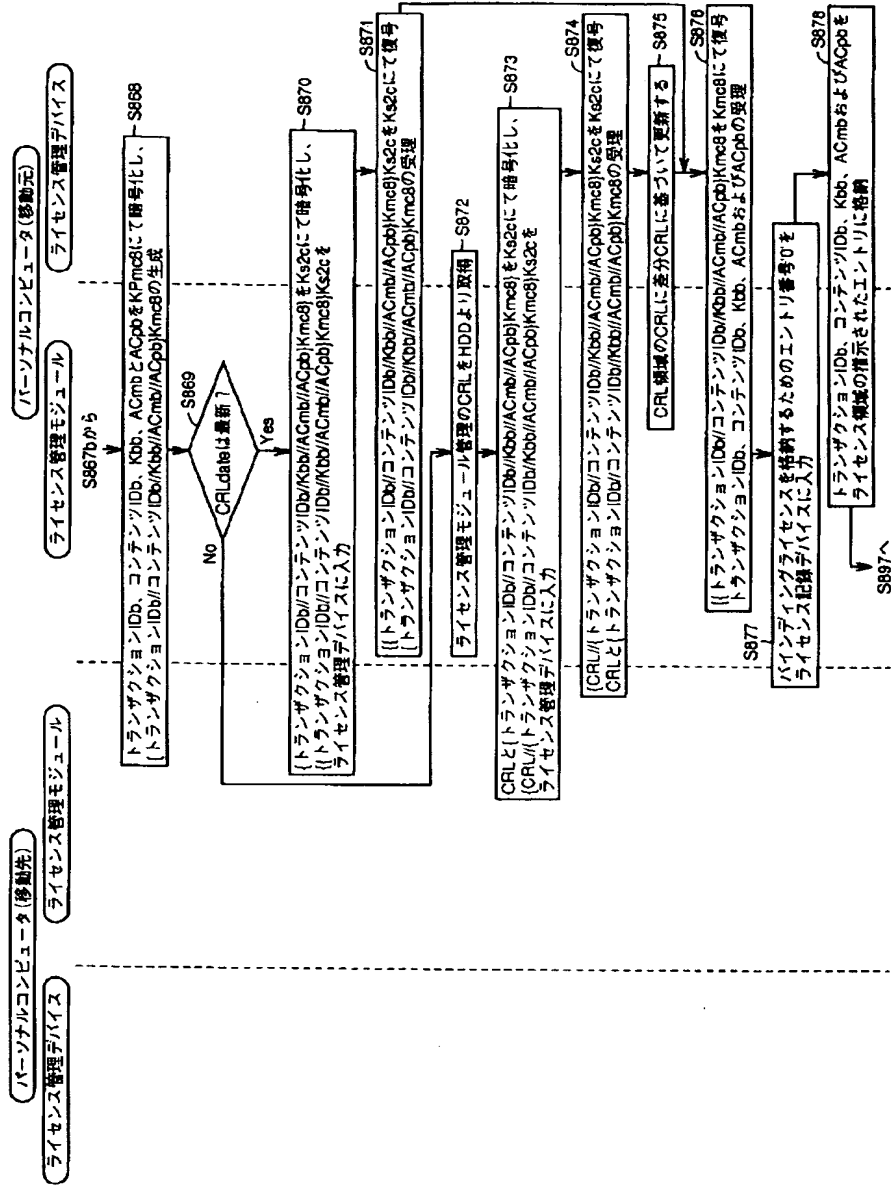
【図71】



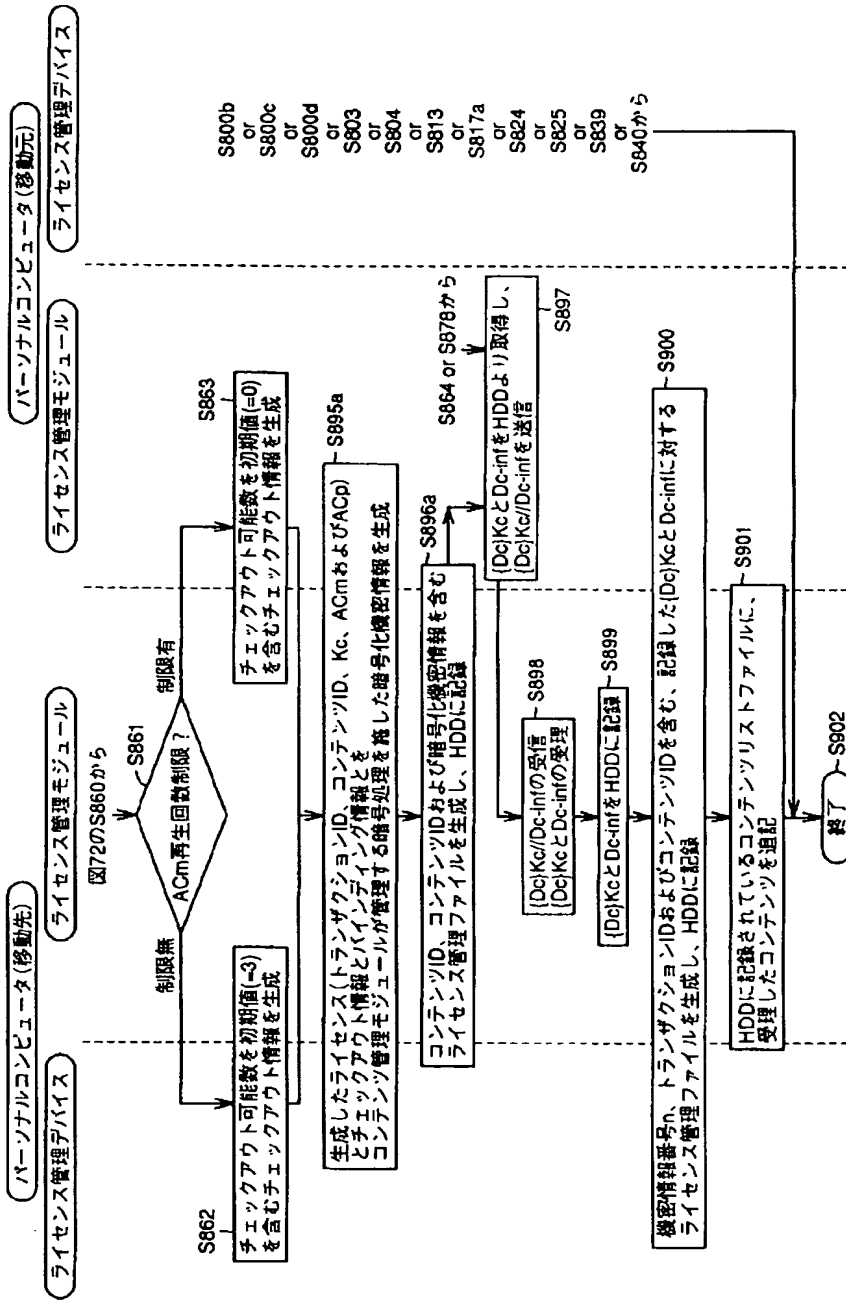
【図72】



【図73】



【図74】



フロントページの続き

(51)Int.Cl.<sup>7</sup>

識別記号

F I  
H 0 4 L 9/00

マークト(参考)

6 0 1 E  
6 7 5 B.

(71)出願人 000005108  
株式会社日立製作所  
東京都千代田区神田駿河台四丁目6番地

(71)出願人 000004167  
日本コロムビア株式会社  
東京都港区赤坂4丁目14番14号

(72)発明者 堀 吉宏  
大阪府守口市京阪本通2丁目5番5号 三  
洋電機株式会社内

(72)発明者 上村 透  
大阪府守口市京阪本通2丁目5番5号 三  
洋電機株式会社内

(72)発明者 畠山 卓久  
神奈川県川崎市中原区上小田中4丁目1番  
1号 富士通株式会社内

(72)発明者 高橋 政孝  
石川県河北郡宇ノ気町字宇野気ヌ98番地の  
2 株式会社ビーエフユー内

(72)発明者 常広 隆司  
神奈川県横浜市戸塚区吉田町292番地 株  
式会社日立製作所システム開発研究所横浜  
ラボラトリ内

(72)発明者 大森 良夫  
神奈川県川崎市川崎区港町5番1号 日本  
コロムビア株式会社川崎工場内

Fターム(参考) 5J104 AA07 AA13 AA15 AA16 EA06  
EA19 KA02 KA05 NA02 NA03  
NA06 NA35 NA37 NA38 NA41  
NA42 PA07 PA11

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT OR DRAWING
- ~~BLURRED~~ OR ILLEGIBLE TEXT OR DRAWING
- SKEWED/SLANTED IMAGES
- COLOR OR BLACK AND WHITE PHOTOGRAPHS
- GRAY SCALE DOCUMENTS
- LINES OR MARKS ON ORIGINAL DOCUMENT
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**